People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
Larbi Tébessi University - Tébessa
Faculty of Exact Sciences and Natural and Life Sciences
Department: Mathematics and Computer Science

Final thesis
For obtaining of the *MASTER* diploma
Domain: Mathematics and Computer Science
Field: Computer Science
Specialty: Systems and Multimedia

HANDWRITTEN DIGIT RECOGNITION USING IMAGE ENCRYPTION

Presented by:

Bouchoucha Mohammed Tayeb

Infront of the jury:

Mr.BennourAkram	MCA Univérsité Larbi Tébessi	President
Mr.Soli Yacine	MAA University LarbiTébessi	Examiner
Mr.GattalAbdeljalil	MCA University Larbi Tébessi	Thesis Supervisor

Date of defense: 13 June / 2020

Abstract

Handwritten digits recognition is a key research problem in the domain of image analysis and pattern recognition. Specifically, the appearance approaches based on feature extraction to solve many research issues. This work presents a novel way to use encryption techniques such as feature extraction stage. Moreover, this method is very efficient for handwritten digit recognition as it is less effected from variations in shape and slant. The proposed method is carried in two steps: first, we concatenate entire image with its encrypted image. Second, the pixels imageis collected into a vector. The performance of the proposed approach is evaluated for recognizing the isolated handwritten digits from the CVL dataset. The experimental results showed recognition with high accuracy.

Keywords: Handwritten digits recognition, encryption techniques, CVL dataset.

Résumé

La reconnaissance des chiffres manuscrits est un problème de recherche clé dans le domaine de l'analyse d'images et de la reconnaissance de formes. Plus précisément, l'apparence s'appuie sur l'extraction de fonctionnalités pour résoudre de nombreux problèmes de recherche. Cette travaille présente une nouvelle façon d'utiliser des techniques de cryptage telles que la phase d'extraction de caractéristiques. De plus, cette méthode est très efficace pour la reconnaissance de chiffres manuscrits car elle est moins affectée par les variations de forme et d'inclinaison. La méthode proposée se déroule en deux étapes : premièrement, nous concaténons l'image entière avec son image cryptée. Deuxièmement, l'image en pixels est collectée dans un vecteur. La performance de l'approche proposée est évaluée pour reconnaître les chiffres manuscrits isolés de base de données CVL. Les résultats expérimentaux ont montré une reconnaissance avec une grande précision.

Mots clés : La reconnaissance des chiffres manuscrits, techniques de cryptage, base de données CVL.

ملخص

يعد التعرف على الأرقام المكتوبة بخط اليد مشكلة بحث رئيسية في مجال تحليل الصور و التعرف على الأنماط. على وجه التحديد, هذا النهج قائم على استخراج المزايا لحل العديد من مسائل البحث. يقدم هذا العمل طريقة فعالة جدا في التعرف على الأرقام المكتوبة بخط اليد لأنها أقل تأثرا للاختلافات في الشكل و الميل. يتم تنفيذ الطريقة المقترحة في خطوتين: أولا, نقوم بجمع الصورة بأكملها مع صورتها المشفرة. ثانيا, يتم تجميع بكسل الصورة في شعاع.يتم تقييم أداء النهج المقترح بالتعرف على الأرقام المعزولة المكتوبة بخط اليد من قاعدة البيانات CVL . أظهرت نتائج التعرف التجريبية دقة عالية.

كلمات مفتاحية: التعرف على الأرقام المكتوبة بخط اليد, تقنيات التشفير, قاعدة البيانات CVL

Table of Contents

Chapter 03: Experimental Results

List of Figures

Chapter 01: Handwritten Digit Recognition System

Chapter 02: Image Encryption Techniques

Chapter 03: Experimental Results

List of Tables

Chapter 03: Experimental Results

General Introduction

General Introduction

Machine Learning (ML) is a method which trains the machine to do the job by itself without any human interaction. At a high level, ML is the process of teaching a computer system on how to make accurate predictions when fed the data. Those predictions will be the output, the purpose of ML is to sense, remember, learn and recognize like a human being.Advances in ML in the past few years have opened up a reeling array of applications in a wide variety of domains such as Advertising, Finance, Health-care, Security, Autonomous systems, Robotics etc. Breakthroughs in the fields of ML and advances in computational and data storage capabilities have altered the landscape of technology. ML has become so pervasive that it is no longer unknown to most smart phone users that their data is constantly being collected for use by predictive models. With this comes the growing concern regarding user data privacy. This has also led to the understanding that ML creates and exposes new vulnerabilities in softwares that use them. For example, the data submitted to the models for prediction could be stolen or misused. Training data used by them could be tampered with, and modified to skew the model in favor of particular outcomes with malicious intent. Attackers could pose as clients to employ the services of the model, and try to steal the model for its intellectual value. Not all data used in these models is sensitive, but in fields like Finance and Health-care, both accuracy and maintaining data privacy become very important. Handwritten Digit Recognition (HDR) has been the main research problem in the document analysis and recognition community for more than three decades. HDR sub-problems mainly include segmentation of lines, words or characters, recognition of single characters, words or complete lines / paragraphs, and recognition of single-digit and string digits.

The aim of this work is using Image Encryption (IE) for improving the performance of HDR system. The choice of HDR systems what determines the accuracy, and for the cryptosystems needs to not only enable processing on encrypted data, but also be secure. The main goal of this work is to perform computations on the encrypted data, preserving the features of both the original image and the encryption. The Relationship between HDR system and cryptosystems is an Inverse Relationship, the more accuracy get higher and closer to the regular system means that we have a great model and a bad cryptosystem and the more accuracy get lower to the regular system means that we have a great cryptosystem and a bad model.

This work mainly focuses on identifying the 10 classes (0-9) from isolated dgits handwritten. The input image is a gray scale image, the intensity level of which varies from 0 to 255. For simplicity, input images should contain only one unknown digit in the middle. In my experimentation I used the Normalized CVL Single Digit dataset which consists of 7000 single digits (700 digits per class) written by approximately 60 different writers. We used many IE systems to encrypt our dataset such RSA Encryption, ECC Encryption, Knight, Chaos, Joseph and Arnold.

General Introduction

The thesis is organized as follows:

In chapter 1, we present the different stages of HDR system including the pre-processing stage, features extraction stage to classification approaches based on Machine Learning techniques.

In the second chapter, we cover the basic theoretical aspects of the IE techniques we used in our work, their vulnerability and how cryptanalysis can penetrate and attack them. This will be useful for justifying the choices made in the HDR system and to explain the results.

In the last chapter, we describe the design and implementation details, models used presents an analysis of the experiments with the different IE techniques and their results.

The work ends with a conclusion on the results obtained by the used methods, and future works which will show the possible evolutions of this work.

Chapter 1

Handwritten Digit Recognition System

Chapter 01: Handwritten Digit Recognition System

1 Introduction

For several decades handwritten recognition has been a traditional field that has attracted the attention of researchers and remains a very open field of research due to its large number of practical applications. Today, the advances made in this area are reflected in a number of applications such as the automatic reading of bank checks, postal addresses and form addresses. The Handwritten Digit Recognition (HDR) system is considered an initial point in the field of pattern recognition and it becomes a major research topic.
In this chapter, we present the different stages of Handwritten Digit Recognition (HDR), emphasizing all the stages of the system of HDR.

2 Types of Handwritten Digit Recognition

The first step in HDR system which makes it possible to recognize any digit in any format consists in converting the writing into numerical values suited to the processing system with a minimum of possible degradations. It all depends on the type of acquisition devices and processed data and of course the intended application. There are several modes of HDR systems according to the of acquisition mode [1]

- ❖ Online recognition systems
- ❖ Offline recognition systems

These are two different Types of HDRs, each with its own acquisition tools and its corresponding recognition algorithms.

2.1 Online recognition systems

This type is also called dynamic. Online writing recognition is carried out in real time, that is to say it is carried out during character tracing, which makes it possible to obtain a good correction and modification according to the response given to the recognition stage integrated with the acquisition stage.

There are many online input methods such as the Graphics Tablet with a digital pens and the touch screen are commonly used.

2.2 Offline recognition systems

This type is also called static where the information is presented in the form of a set of pixels which represents the image of an already existing text, obtained by a scanner or a camera. Recognition of offline writing is more complex than that of online writing due to the presence of noise in the image acquisition process and the loss of temporal information such as such as the temporal order of the points as well as the speed of the pen can be used by the recognition system, this type introduces an additional difficulty relating to the variability of the thickness and connectivity, requiring the application of preprocessing techniques.

The fields of application are diverse and mainly concern the automatic processing of postal addresses, bank checks, forms, digital identifiers, process sheets, etc.

3 The system of HDR

The system of HDR has become an interesting field that attracts researchers in the decade preceding years. The recognition system based on Machine Learning techniques is composed of five important stages.
Acquisition, pre-processing, segmentation, features extraction and classification (See "Figure 1.1):

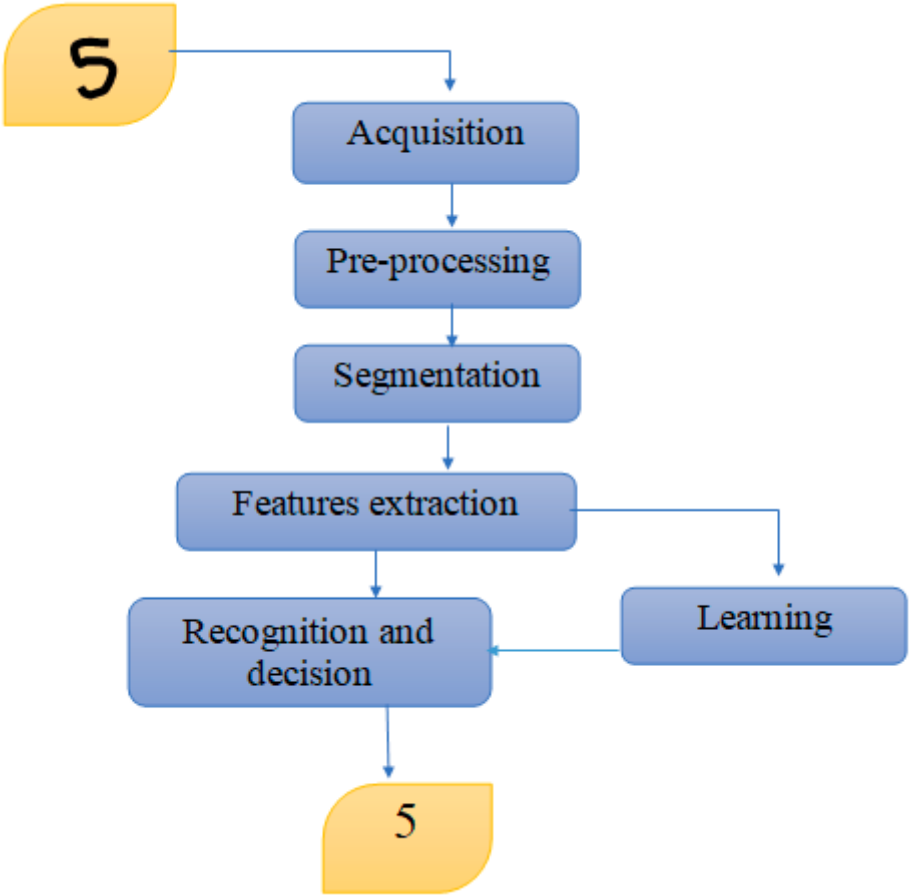

Figure 1.1: General diagram of a HDR system.

3.1 Acquisition stage

The acquisition stage is essentially based on capturing the image of handwriting using physical sensors and converting it into digital elevations adapted to the computerized processing system with a minimum possible degradation.
If the information is available on paper often, physical sensors are scanners or digital cameras. During this stage, despite the good quality of the acquisition systems, parasitic noise may

appear and cause background heterogeneity [2]. This is due to the nature of the texture, the work area and its lighting.

3.2 Pre-processing stage

Pre-processing is the first and key step in HDR. It affects the implementation of recognition algorithms.
The objectives of pre-processing stages are numerous. It is mainly used to reduce noise on handwritten data, sometimes to correct faults, and try to keep only the important information from the representative form.
The pre-processing plays a very important task and can directly influence the performance of the recognition, since there are many steps to complete the recognition successfully, we can quote them below:

3.2.1 Noise reduction

Noise reduction including mainly dropping, smoothing and correction of the wild point, characterized by large angular variations as described in the paper in [3]. This is to eliminate the maximum noise to increase discrimination. See “Figure 1.2”:

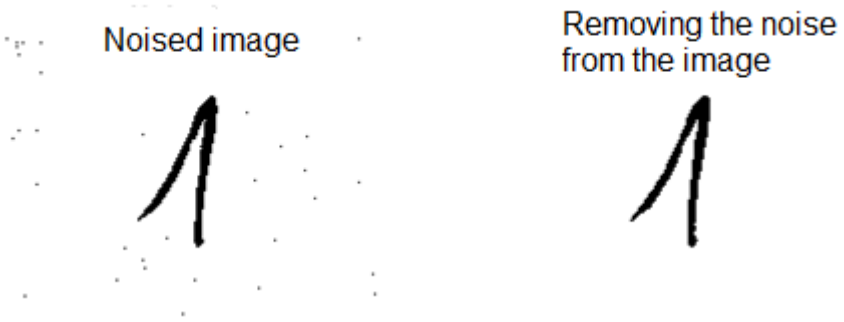

Figure 1.2: Example of Example of noise removal.

3.2.2 Binarization

The Binarization method converts the grey scale image (0 up to 255 gray levels) in to black and white image (0 or 1). The result of the recognition highly depends upon the binarization. The high quality binarized image can give more accuracy in HDR as compared original image because noise is present in the original image [4].

The selection of most optimal binarization algorithm is difficult, because different binarization algorithm gives different performance on different data sets. This is especially true in the case of historical documents images with variation in contrast and illumination. The algorithms divide into two categories [5]:

a) Global Binarization: Methods used single threshold value for whole image, like Otsu method and Kittler method.

b) Local Binarization: Methods where the threshold value calculated locally pixel by pixel or region by region, like Niblack method and Adaptive method.

Figure 1.3: Convert image to binary image.

3.2.3 Skeletonization

Skeletonization and also known as thinning process is an important step in pre-processing stage. Skeletonization is a crucial process for many applications such as OCR, writer identification ...ect.[6].

The skeletonization process makes it possible to reduce and compact the size of the image, to keep the general shape of the particle and to find a median axis, defined as the set of pixels S which have an equality of distance with respect to the border pixels. surrounding them [7]. Skeletal representation has the following advantages [7]:

- A good way to best represent the structural relationships between model components.
- Widely used in character, word, signature and imprint recognition systems.

Figure 1.4: Example of skeletonization.

3.2.4 Size normalization

To facilitate the recognition stage, the digits need to be normalized to a fixed size using sampling techniques. This is why Size normalization is an important pre-processing technique in character recognition.
The primary constraint lies in the choice of this size. The excessively small size has a risk of loss of information. Too large, the recognition stage will operate slowly [8].

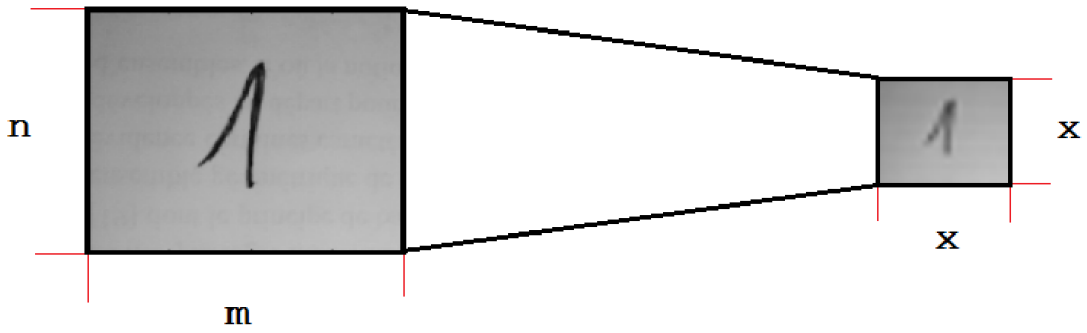

Figure 1.5: Example of normalized handwritten digit.

3.2.5 Zoning

In the process of recognizing handwritten character, image zoning is a mostly used technique for extracting special features from pattern. Zoning is able to handle variation in handwritten pattern, which is due to different physical and psychological conditions of writer.

When resizing an individual image of size "nxn", the pixels are divided into equal areas or blocks, each of which is the same size. The features are extracted by counting the number of black pixels in each area. This procedure is repeated sequentially for all the areas

which are stored in the form of a vector for each character. Thus, for each character, we obtain an array calculated from each area [9].

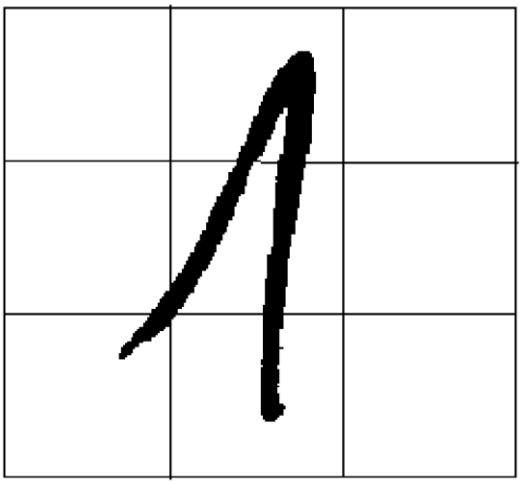

Figure 1.6: Example of zoned digit with size (3*3).

3.3 Segmentation stage

Image segmentation is the fundamental approach and the most important part in image processing [10], Segmentation divides the handwritten text into several entities such as words and digits. For the segmentation of the handwritten digits, this consists of dividing the string of digits into several images, each comprising an isolated digit. Likewise, for literal images. There are two main categories of segmentation:

- ❖ Explicit segmentation
- ❖ Implicit segmentation

3.3.1 Explicit segmentation

In this approach, the separation of the digits consists in dividing the string of the digits in several images perfectly as possible, see "figure 1.7".
The segmentation paths are generally obtained by characteristic points, such as [11]:

✓Local minima of the upper contour.

✓Spaces between characters or sub words.

✓ The most likely intersection points by an analysis of the components in the word.

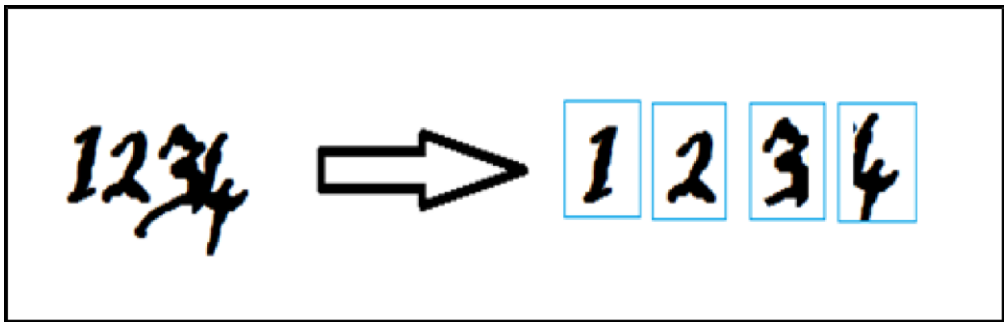

Figure 1.7: Example of segmentation of handwritten digits (explicit).

3.3.2 Implicit segmentation

Implicit segmentation consists in segmenting the string into different parts of the digits called graphemes and finding the digits and then the string by combining these graphemes [11], See "Figure 1.8".

This segmentation has advantages and disadvantages which makes this approach insufficient for optimal modeling of writing [11]:

✓ The advantage of this segmentation is that the information is localized by the models of the letters and the validation is done by its models. There will be no segmentation error and finally we get around Sayre's dilemma because by knowing the letters, we do not generate segmentation error.

✓ The shortcomings of this segmentation come from the fact that the searching space for the limits is greatly increased and the problem is reduced to a problem of searching for areas where these limits are found.

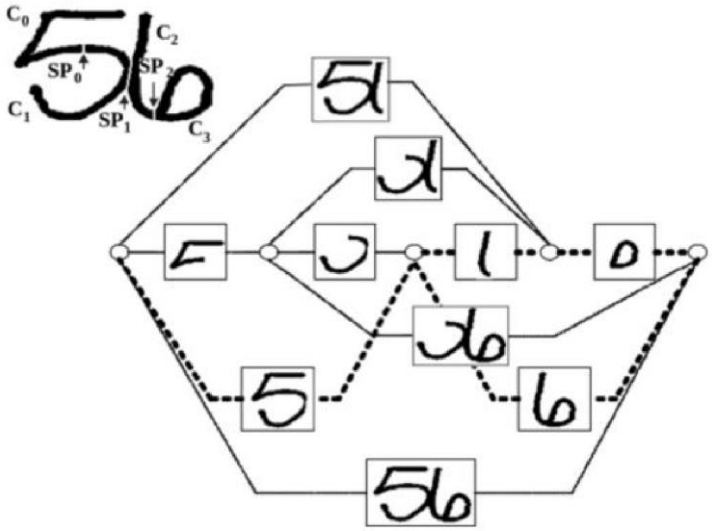

Figure 1.8: Example of segmentation of handwritten digits (implicit).

3.4 Features extraction stage

The purpose of feature extraction in the recognition field is to express the primitives/features in a numeric or symbolic form called coding. Depending on the case, the values of these features can be real, integer or binary [12].

The difficulty here is to find good features. "Good" features allow classifiers to easily recognize different classes of objects; we then say that they are discriminating. They must also be invariant to certain transformations "the number 1 belongs to the same class whatever the size and structure" [13].

3.4.1 Structural features

The structural features of the image which may consider the character shape example contour, end point, branch points, loops, directions and others [14].
A structural description of a texture involves the search for elementary patterns, their description, then the determination of the rules conditioning their position [15]. In general, the structural features used depend on the form and the shape to be classified.

3.4.2 Textural features

Texture analysis refers to the characterization of the regions of an image by their texture content. Texture analysis attempts to quantify the intuitive qualities described by terms such as rough, smooth, silky or bumpy, depending on the spatial variation of the pixel intensity. In this sense, roughness or bumps refer to variations in intensity values, or gray levels.

3.4.3 Global features

Global features combine long-range model information into a one feature value. To best represent the general character form , depend on the totality of the pixels of an image, these features are therefore derived from the distribution of the pixels [16].
Global features seek to best represent the general character form, therefore they are calculated on relatively large images "ex: Fourier transform and Hough transform" [17].

3.4.4 Morphological features

The mathematical morphology makes it possible to extract a skeleton pixel which guarantees the connectivity of the initial image [18].Mathematical morphology is Image Analysis Technique and can be used to solve a large number of image processing problems such as [19]:

✓**Non-linear filtering of images**: To preserve or delete structures from an image having certain features, in particular of "morphological" form.

✓**Segmentation:** To obtain a partition of the image into its different interest regions. Generally, the segmentation try to separate objects from the background image. The morphological segmentation paradigm is based on the watershed operator.

3.5 Classification stage

Classification is the elaboration of a decision rule which transforms the attributes characterizing the forms belonging to a class "passage from the coding space to the decision space" [20]. According to [21], The classification process is carried out in two stages:

3.5.1 Learning

This step allows to build a prototype dictionary. It is a question of regrouping/clustering in classes several prototypes whose features are similar. According to [22], there are three types of learning:

3.5.1.1 Supervised learning « *Classification* »

Supervised learning “or classification” consists of building a model based on a learning dataset and Labels “classes” and using it to classify new data [23] [24]. There are several algorithms and techniques used for supervised classification such as:

- K-Nearest Neighbors (KNN)
- Bayesian classification.
- Support Vector Machine (SVM).
- Artificial Neural Networks (ANN).
- Decision tree.

3.5.1.2 Unsupervised learning

Unsupervised learning consists in providing the system with an automatic mechanism which relies on precise grouping rules to find reference classes with minimal assistance. In this case the samples are introduced in large numbers by the user without indicating their class [25].

There are several clustering algorithms, for example:

- Artificial Neural Networks "ANN"
- K-means “KMeans”
- Fuzzy K-Means
- Hierarchical clustering

3.5.1.3 Semi-supervised learning

Semi-supervised learning uses labeled and unlabeled dataset. It therefore falls between supervised learning which uses only labeled data and unsupervised learning which uses only unlabeled data. The use of unlabeled data, in combination with labeled data, can significantly improve the quality of learning. Another advantage comes from the fact that the data tag (labeled) requires the intervention of a human user. When the datasets become very large, this

operation can be tedious. In this case, semi-supervised learning, which requires only a few labels, is of obvious and indisputable practical interest [26]. In the case of the recognition of handwritten digits, the supervised classification was adopted because it considerably simplifies the problem [27].

3.5.2 Recognition and decision

Recognition can lead to success if the answer is unique "only one model meets the description of the character shape ". It can lead to confusion if the answer is multiple "several models correspond to the description". Finally, it can lead to a rejection of the shape if no model corresponds to its description. In the first two cases, the decision may be accompanied by a likelihood measure, also called a score or recognition rate [28]. According to [29], there are three main approaches and a hybrid approach:

3.5.2.1 Statistical approach

In this approach, recognition is based on the statistical study of the measurements that are made on the forms to be recognized [30]. But it needs a large number of samples to correctly learn the probability laws of the different classes. The study of their distribution in a metric space and the statistical characterization of the classes makes it possible to make a decision of the type: higher probability of belonging to a class. This approach benefits from machine learning methods which are based on known theoretical bases such as:

✓ Parametric methods (Bayes' rule, neural networks, Markov chains, etc.) [31]

✓ Non-parametric methods (k nearest neighbor method, etc.) [32]

3.5.2.2 Stochastic approach

The stochastic approach uses a model for recognition, taking into account the great variability of the shape. In this type of approach, the models are often discrete and many works are based on Markov chain and Bayesian estimation.
Markov fields are used to reduce global properties to local constraints. The model describes these states using probabilities of state transitions and probabilities of observation by state [33]. The comparison consists in searching in this state graph, the path of high probability corresponding to a series of elements observed in the input chain. [34]. The most popular methods in this approach are the methods using Hidden Markov Models (HMM).

3.5.2.3 Hybrid approach

To improve recognition performance, the trend today is to build hybrid systems that use different types of features, and that combine several classifiers in layers. to overcome the weaknesses of each approach and obtain more precise results more better than the results that would have been obtained if the application of each approach separately, such as the approaches that were merged to form the integrated one [1].

An example of this approach a hybrid approach which combines statistical and structural approaches.

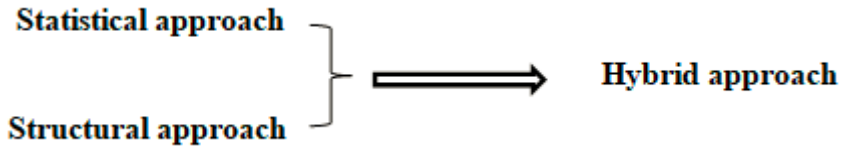

Figure 1.9: Example of hybridization between two approaches (statistical and structural).

4 Statistical classification methods

The statistical approach has been chosen for the recognition of digits which are based on theoretical bases such as parametric methods. Among the classification methods that have been developed in this context (machine learning), we distinguish for example neural networks and support vector machines (SVM) as well as K-nearest neighbors (KNN) [35].

4.1 Neural Networks

Neural networks[36] is a rather vague name which covers a set of calculation mechanisms initially inspired by models from the functioning of nervous systems that technicians see there as a source of inspiration for the construction of automatic systems [12].
A great effort has been devoted to the development of Neural Networks which present an alternative to classical architectures. This is due to their parallel structures, their Classification performance and their ability to understand nonlinear phenomena.
Mainly a Neural network only works after having learned enough knowledge about the desired outputs from given inputs; the development of these networks mainly concerns learning and the laws of modification of connection weights. [36].

4.2 K-Nearest Neighbors (KNN)

The K Nearest Neighbors classifier It is a simple classifier based on the calculation of distance between learning examples and test examples, generally the Euclidean standard is often used as a distance measure, in each learning step [37], the algorithm stores the k best examples of the learning set (KNN) which are close to the test sample. This algorithm is often efficient if there are enough learning examples, but requires a very long prediction time to pass all the samples in order to find the K best solutions [38] [39].

4.3 Support Vector Machine (SVM)

SVMs are a set of supervised learning techniques intended to solve problems of binary classification and regression. SVMs are based on two ideas, the maximum margin and the the kernel function.

The maximum margin is used for the problems of linear classification. It represents the distance between the separation boundary and the closest learning samples. These are the support vectors.

The kernel functions are used in the case of the problems of the non-linear classification to transform the space of representation of the input data into a space of larger dimension in which it is probable that there exist linear separators [40].

The SVM classifier is an algorithm that maximizes the margin between the classes of the problem to be solved and minimizes the classification error. The objective of the maximum margin is to have two classes separated by a hyperplane so that the distance from the support vectors is maximum [41].

In the classification task, an SVM builds the optimal hyperplane for the separation of characteristic attributes in a high dimensional space [42]. The calculation of this hyperplane is based on the maximization of the margin between the closest learning samples which belong to different classes.

5 Conclusion

In this chapter, we have presented in general the different stages of the HDR system, from the acquisition stage to classification approaches based on machine learning techniques. In the second chapter, we will have addressed the main methods of image encryption.

Chapter 2

Image Encryption Techniques

Chapter 02: Image Encryption Techniques

1 Introduction

Cryptanalysis plays a major role among the cryptographic areas of research. Nowadays cryptanalysis technique plays equal opposite directions of cryptosystems. Due to some little bit of weakness; every cryptosystem has a breakable one in somehow.This chapter fully cares about current cryptanalysis research of some cryptosystems (RSA, ECC and Some traditional image encryption such as Arnold, chaos and knight).

2 Cryptology

Cryptology the « science of the secret» is a mathematical science that has two branches: cryptography and cryptanalysis [43].

2.1 Cryptography

Cryptography is a science making it possible to convert information "in clear" into coded or encrypted information, i.e. not comprehensible, then, starting from this coded information, to restore the original information (information in clear) [44].
The goal of cryptography is to design a system (cryptosystem) whose only known attack is exhaustive research.

2.1.1 Cryptosystem

Cryptosystem is a suite of cryptographic algorithms needed to implement a particular security service, most commonly for achieving confidentiality [45].

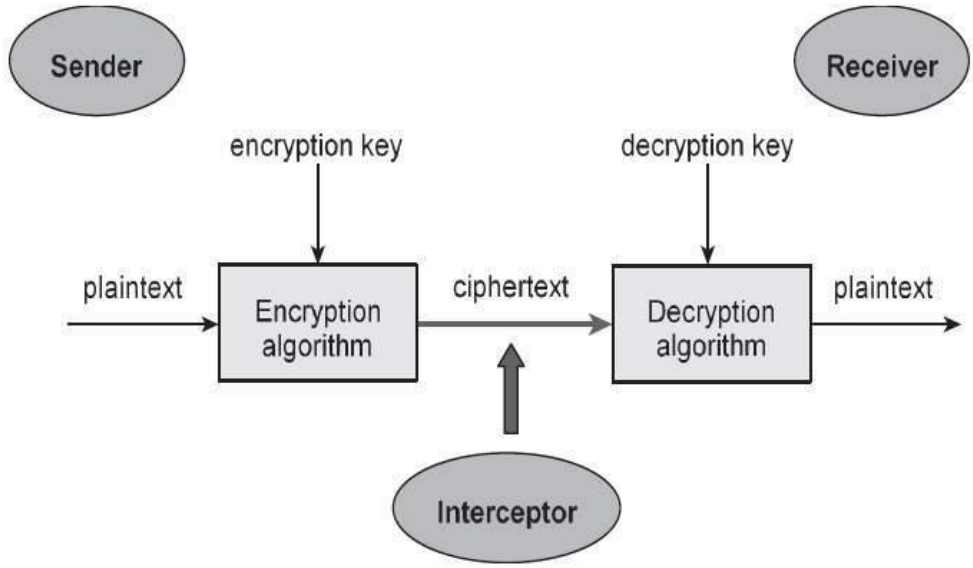

Figure 2.1: Cryptosystem schema.

There are two main cryptography systems:

Symmetric Cryptography is a cryptographic system that uses the same cryptographic keys for both encryption of plaintext and decryption of ciphertext (AES, DES, RC4…). The keys may be identical or there may be a simple transformation to go between the two keys [46]. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link [47].

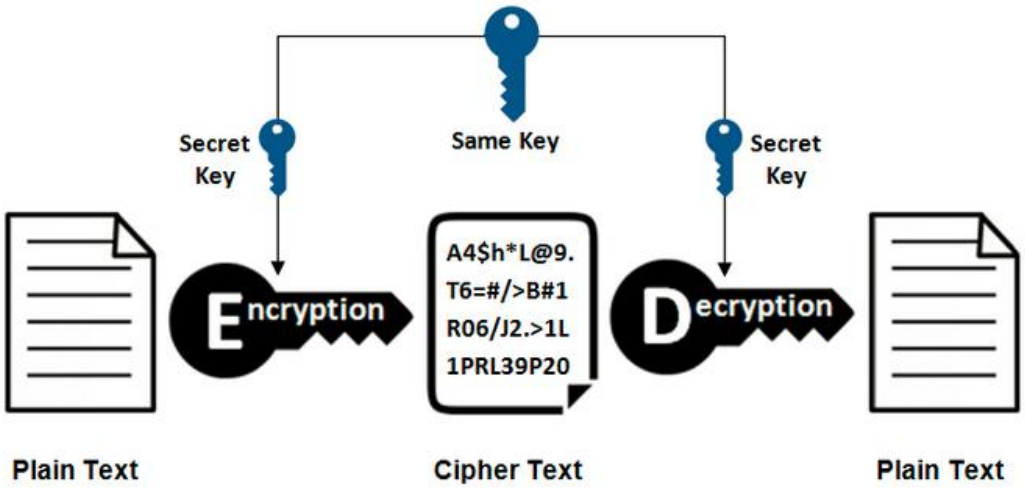

Figure 2.2: Symmetric Cryptography.

Asymmetric Cryptography is a cryptographic system that uses pairs of keys: public keys, which may be disseminated widely, and private keys, which are known only to the owner (RSA, ECC…). The generation of such keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.[48]

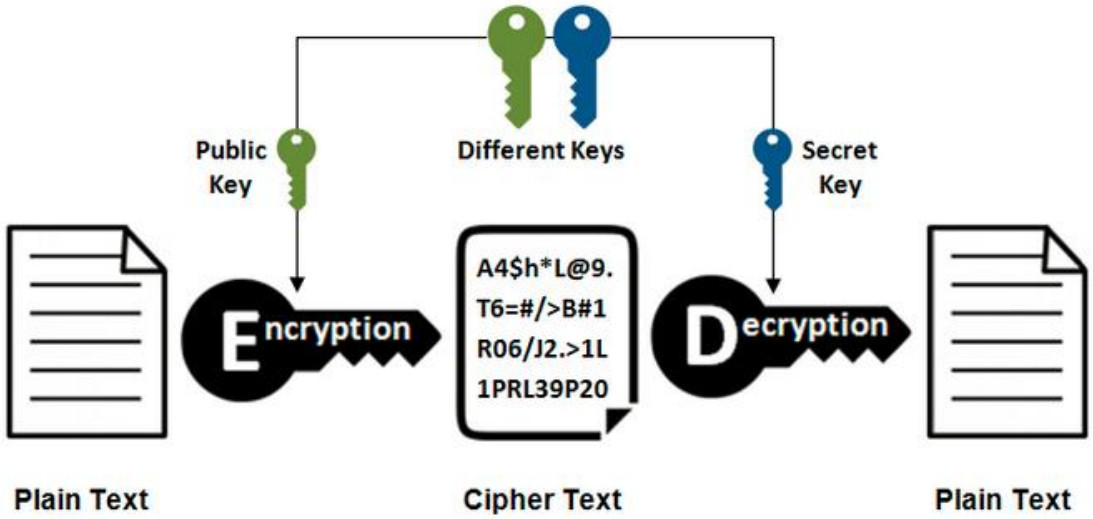

Figure 2.3: Asymmetric Cryptography.

Some cryptosystem examples:

2.1.1.1 RSA Encryption

RSA is one of the first public-key cryptosystems and is widely used for secure data transmission. It is an asymmetric cryptographic algorithm. It uses two different keys, a public key known to everyone while the private is kept as a secret. The authorized users only know how to open the message. The encryption ratio of RSA algorithm is high and processing speed is also fast. The key length of this algorithm is more than 1024 bits. Block size of RSA

algorithm is 446 bytes and 1 round for encryption. RSA is implemented using a stream cipher. The loss will arise while decrypting the data. Three different operations used to fulfill the encryption process: Key Generation, Encryption and Decryption [49].

Key Generation
Step 1: Choose two different prime numbers randomly, name as p and q
Step 2: Multiply these two prime numbers and the results stored in variable n. (n= P*q)
Step 3: Calculate the value of φ (n) = φ (p) φ (q)
Step 4: Select an integer e such that 1<e<φ (n) and calculate the greatest common divisor between the integer e and φ (n). These gcd value is should equal to 1 (gcd (e, φ (n)) =1).
Step5: Calculate the value of d, such that d= e-1 mod φ (n).

Encryption
Step 6: Sender transmits public key (n,e) to the receiver and kept d(private) as secret.
Step 7: Receiver sends message M to the sender in the form of c= me mod n.

Decryption
Step 8: Sender can recover message from cipher text with the help of private key d
Step9: d is calculated through the form of, m= cd mod n.

In an encrypted image, no one can view the data or the original image there. To view the original data or image

.

Figure 2.4: Normalized digit (0) encryption with RSA.

2.1.1.2 ECC Encryption

Elliptic curve cryptography (ECC) ispublic-key cryptosystem and a widely-used technique in multi-factor authentication [50]. ECC is a public key encryption technique based on elliptic curve theory that can be used to create smaller keys, which yields faster and more efficient algorithms as a result. It generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product ofvery large prime numbers. It provides significantly more security than first-generation public key cryptography systems like RSA [51].
ECC utilizes the mathematics of elliptic curves. The security of ECC lies in the complexity of working the elliptic curve discrete logarithm problem. An analysis of ECC theory and its computational problems are stated below.

As shown in Figure 2.5, elliptic curves (Eq (a, b)) are a set of points defined by the solutions to the equation $y^2 = x^3 + ax + b$ (mod q), where a and b are elements of the field k together with a point at infinity **O**. There is also a condition such that $4a^3 + 27b^3 \neq 0$ (mod q) where q is

a prime number. This equation must be satisfied for the elliptic curve to have a well-defined group structure. This forms an additive cyclic group E = {(x, y)∈ Eq (a, b)}∪ {**O**}, where **O** serves as an additive identity element of the group [57]. If P is a point in E and k is a positive integer, then the point multiplication is computed by repeated addition, such as k. P = P + P …+P, where k is a large integer and P is added to itself k times.

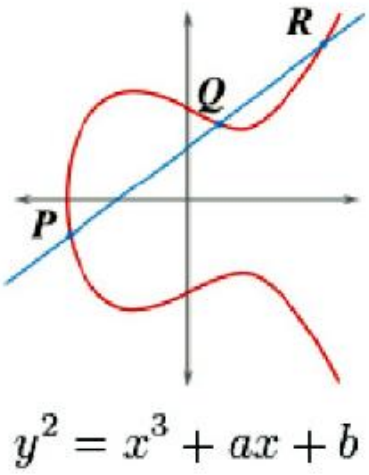

Figure 2.5: Ellipitic curve addition.

Figure 2.6: Normalized digit (0) encryption with ECC.

2.1.1.3 Chaos Encryption

Chaos theory is field of study in mathematics that studiesthe dynamic systems behavior and condition that are highly sensitive to initial condition. Slight change in initial condition leads to widely diverging output. In other words, if chaos system is used for image scrambling then without knowledge of initial condition (here it is scrambling key) one may not be able to descramble the image from input scrambled image. There are many chaotic maps which are used for generating chaotic sequence. One of them is Logistic map. Logistic map isa polynomial mapping in which chaotic behavior is generated by nonlinear dynamic equation given in the equation. Logistic map is given by:

$$x(n+1) = \mu x_n(1 - x_n) \qquad (1)$$

Where, $0 < x_n < 1$ where, n = {0,1,,N}, withx_0 = initial condition; and
μ= Bifurcationparameter: To get chaotic behavior from Logistic map [52] value of μ must be in range $3.5699456 < \mu < 4$. Algorithm for image scrambling using Logistic map is as follows: Consider an image I of size is M x N and (i; j) represent the pixel coordinates, i = (1,2,,M) and j = (1, 2,, N)

1) Generate chaotic sequence, Sq, of length M x N usingequation7. Values of x_0 ,μ can be used as scrambling key.

2) Scale the chaotic sequence values from range 0 <Sq<1 to the range 0 <Sq'< 255.
3) Create 2D array R(i; j) of sizeM x N from 1D sequenceSq'.
4) Perform EX-OR operation which is reversible operation; on pixel values and array R (i; j) to get pixel value transformed image I'.
$I'(i; j) = I(i; j) \oplus R(i; j)$
5) Apply a scrambling algorithm to get final scrambled image.
To descramble the image, key = $\{x_0; \mu\}$ is needed.

Figure 2.7: Normalized digit (0) encryption with Chaos.

2.1.1.4 Knight Encryption

Knight's Tour Problem (KTP) is one of the oldest problems in chess and computer algorithms. The puzzle is all about moving the Knight throughout the chessboard of dimension (8 x 8) in 63 moves covering each square only single time.
According to Leonhard Euler [53], Knight's Tour Problem on a chessboard of dimension 8x8 pixels can be solved if the following conditions are fulfilled:
The values present in squares, on both the sides of the line joining the centers between them, should have the difference of 32. Half of the total values present should lie on one side of the chessboard and rest on the other side.

A knight's tour path(circuit)can be denoted by a matrix **T**(Fig.2.8) which we call knight's tour matrix as follow: where**1**denotes the starting square of tour,**64** denotes the end square of the tour, ***i*** denotes the location on the board by knight's ***i***thmove.We call the path from 1 to 64 Hamiltonianpath (Hpath). Particularly if there are a legal move from starting squareto end square, we call the path Hamiltonian circuit(H-circuit).

54	5	36	33	56	29	26	31
35	16	55	6	37	32	13	28
4	53	34	57	14	27	30	25
17	58	15	38	7	12	63	40
52	3	18	47	62	39	24	11
59	48	51	8	21	64	41	44
50	19	2	61	46	43	10	23
1	60	49	20	9	22	45	42

28	9	30	13	26	11	34	53
61	14	27	10	31	54	25	36
8	29	62	55	12	35	52	33
3	60	15	6	47	32	37	24
16	7	4	63	56	23	46	51
59	2	19	48	5	40	43	38
20	17	64	57	22	45	50	41
1	58	21	18	49	42	39	44

Figure 2.8: Knight's Tour Matrix.

KTP has always H-path on $n \times n$ chessboard if summation of starting-square's horizontal and vertical location is even when $n \geq 5$ and n isodd.And if $n \geq 6$ and n is even, KTP has always H-path fromeach square.So, we can draw a conclusion that: knight's tour matrix is almost present extensively [54].
There are approximately 1.305×1035 [55] different paths or matrixes (considering the path's symmetry) on 8×8 chessboard.Clearly,it is imaginable that the number for more than 8×8 chessboard is astronomical. So far there has been no documents reporting the lower number for largerboard.But we can make certain that knight's tour path's number on large board is definitely out and away larger than the number on the 8×8 chessboard. In fact, knight's tour path's number on 8×8 chessboard has been already out and away more than the number of Hilbert curve,Peanoapproach, Ecurve,Magic scrambling approach and so on. Sureenough,ithappens that the encryption effects are resemble by fewerknight's tour matrices.But it is impossible to decrypt without the same encryption effect. In addition,the probability of having each same pixel between two cipher images is rather little.Thus, they have nearly little influence to secret key space.In this case, The key space is sufficiently huge using knight's tour matrix.

We consider original image $\mathbf{I} = \{\mathbf{I}_{i,j}\}_{m \times n}$as an $m \times n$chessboard, produce a knight's tour matrix on the board labeledas $\mathbf{T}=\{\mathbf{T}_{i,j}\}_{m \times n}$,called knight's tour slip matrix **T**. Similarly,weproduce a $(2k+1) \times (2k+1)$ knight's tour matrix$\mathbf{A}=\{\mathbf{A}_{i,j}\}_{(2k+1)\times(2k+1)}$($k \geq 2$).For the sake ofdecrypting the cipher image accurately, we emend matrix **A**,and let $\mathbf{A}_{k,k}=1$,label the matrix **A**emended **A**
Then we use the matrix **A**' as a filter templatecalled slip encryption-filter template matrix(encryption-filtertemplate matrix below),and give a name to this filter:slipencryption-filter(encryption-filter below).Now let the center ofencryption-filter template matrix $\mathbf{A'}_{k,k}$move along with thetour path of knight's tour slip matrix **T** and do the convolvsionoperation as the image convolvsionfilter,attain the cipherimage $\mathbf{I'} = \{\mathbf{I'}_{i,j}\}_{m \times n}$

Figure 2.9: Normalized digit (0) encryption with Knight.

2.1.1.5 Arnold Encryption

The transformation of Arnold is the most used in techniques for mixing digital images. Because of this cyclical change, the safety problem, frequent repetition, higher scrambling and therefore the speed or the noise, efficiency is less. In addition, the degree of randomization in the different frequency step is unstable, andsometimes, things get worse, and it is also a hidden security problem [56]. We can outlineArnold's transformation as follows. Let (x, y) inform within the unit sq. It moves tothe (x', y') by the subsequent equation [1 1].

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ 1 \qquad (2)$$

L is the length of a square unit. This conversion called Arnold's 2D conversion. For digital images, Arnold's transformation can be defined as follows. Using the next transformation [57], move the pixels of the square digital image $I = [I\ i, j]_{NXN}$ to(i, j).

$$\begin{bmatrix} i \\ j \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} mod\ N \qquad (3)$$

Arnold's transformation is cyclical and reversible. Moreover, Arnold's transformation is only valid for square images. The Arnold's transformation is used to modify the parameters of digital images, especially for digital watermarks. Many articles believe Arnold's conversion period is <*N*2. However, the article provides a linear approximation of the Arnold amount akin to Equation three as in [1 1].

$$T = 1.4938N + 40.8689 \qquad (4)$$
$$2 \leq N \leq 2000$$

According to the transformation conception of Arnold, the encryption of the position area primarily corresponds to the initial position of the pixels of the captive image. The degree of interference is larger if the constituent moves farther than the constituent of the first image. Encryption does not modify the gray level of the pixels of the first image; however, you will modify the image of the visual result.

Figure 2.10: Normalized digit (0) encryption with Arnold.

2.1.1.6 Joseph Encryption

The Josephus problem is a mathematical application problem and is described as follows: known n individuals (numbered 1, 2, …, n), sitting around a big round table, starting from 1 with the number S, reporting at an interval of g, and the number of people who reported to the end number automatically Then his next one starts counting again from 1 and the interval between the numbers is g, and the number of people who reported to the finish line goes out; so the cycle continues until all the people at the round table are out. For ease of description, define the Joseph function asJosephus (a [], L, S, g, No)
Among them, a[] represents the original sequence, L represents the length of the sequence, S represents the position of the starting report ($1 \leq S \leq L$), g represents the interval of the report number, and No represents the report value of the dequeued position during traversal ($1 \leq No \leq L$). We verify the static and dynamic Joseph ring scrambling.

Figure shows the image contrast effect of Joseph scrambling and row and column swap scrambling on Lena grayscale images of size $256 * 256$. The results show that the effect of Joseph scrambling is better than the effect of common row and column scrambling. However, it can still be seen that there is a certain linear transformation feature, and the scrambled sequence retains part of the linear information features.

Figure 2.11: Normalized digit (0) encryption with Joseph.

3 Conclusion

In this chapter, we described cryptology and its two branches cryptography and cryptanalysis with the main methods of image encryption. In the next chapter we will see the final results of our work.

Chapter 3

Experimental Results

Chapter 03: Experimental Results

1 Introduction

Automated off-line handwritten digits recognition is one of the most researched problems in classical pattern recognition. It has applications in several industries such as handwritten postal codes recognition, processing bank check amounts, storing handwritings based on handwritten numeric entries etc. In this context, the main challenges in recognizing handwritten digit arise from different writing styles, varying font sizes, directions, widths, arrangements, and measurements.

Generally, the feature extraction methods for digit recognition have commonly exploited three types of features: statistical, structural and textual. In this work, we try to replace extraction features stage by image encryption techniques are directly derived from the input images.

2 Development Tools

2.1 Material

- The material used is a Personal Computer:
- Processor: Intel® Core™ i5-6200U CPU @ 2.30GHz 2.40GHz
- Installed Memory (RAM): 8.00 Go
- System type: Operating system Windows 10 Professional, 64 bits processor x64

2.2 Development environment (Matlab)

MATLAB (*matrix laboratory*) is a multi-paradigm numerical computing environment and proprietary programming language developed by MathWorks. MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages.

3 Proposed System

The used image encryption techniques (Knight, Joseph, Chaos, Arnold, RSA and ECC) have been proven to be a powerful measure of image encryption. In its original form, the pixels image of image encryption is collected into a vector that is used as a descriptor. However, the aim of this work is to be able to use an encrypted image of a handwritten digit in the recognition field despite obscuring the shape/structure of the digit and also knowing the ide al encryption method in terms of coding and recognition.

In this section, we first introduce six image encryption techniques to address its limitations in terms of recognition performance. The used encryption technique able to find more structural information over the input image. Therefore, we aim to design the proposed system for recognizing handwritten digits. The schematic diagram of the proposed method is shown in Figure 3.1.

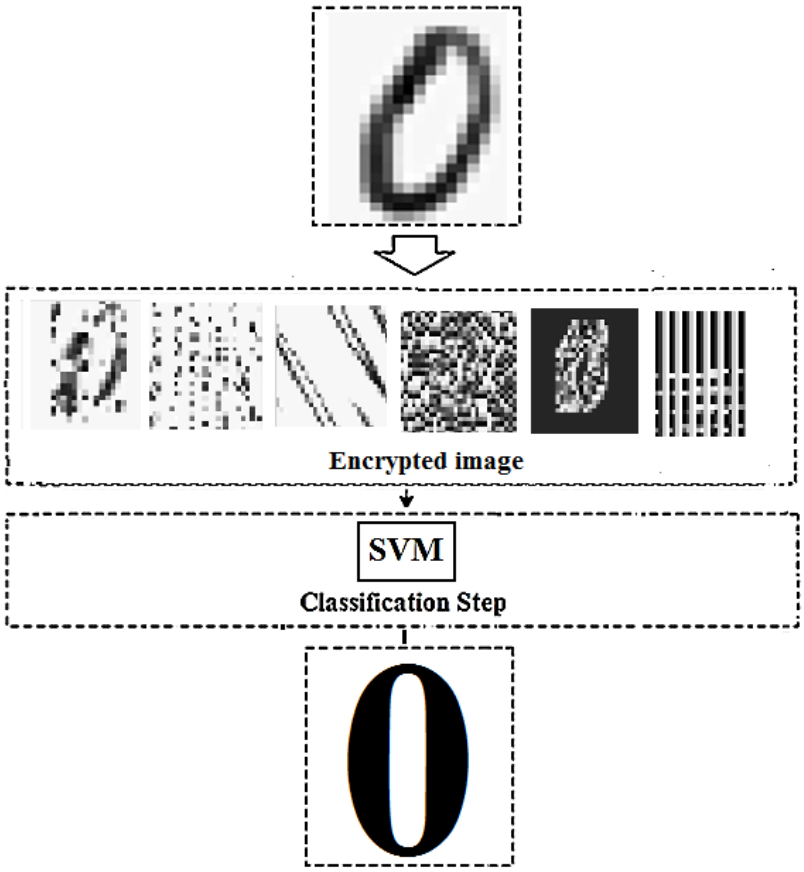

Figure 3.1 Overview of the Proposed System.

3.1 Classification

For the classification task we selected the Support Vector Machine (SVM) as a classifier [76]. The encrypted image is used to train our One-Against-All-based multiclass SVM strategies for 10-digit classes. Two important parameters required for training the SVM include the soft margin parameter (C) and the Radial Basis Function (RBF) kernel parameter (σ).

4 Experimentations and Results

We carried out a series of experiments to evaluate the effectiveness of the proposed system for handwritten digits recognition on the normalized CVL Single Digit dataset [77]. First, all handwritten digits are converted to grayscale images. Next, the encrypted image is encoded the input grayscale image. The dataset comprised 7,000 handwritten digits were provided as a training set and 21,780 as a test set.

Our experiments aim to study the effectiveness of the proposed system used the encryption-based encoding based on six image encryption techniques. The image encryption techniques are generated using Knight, Joseph, Chaos, Arnold, RSA and ECC from the whole image. The system performance is measured using the standard recall measure computed in a similar way as in the ICDAR 2013-digit recognition competition [77].

It can be seen from table 1 that the proposed method based on Arnold technique outperforms the other encryption technique. Table1 summarizes the recall of different encrypted images. A highest recall of 85.99% is achieved making a feature vector of dimension 784.

Table 1. Recall on CVL dataset using different encrypted image.

Used Image		**Dim**	**Recall (%)**
Grayscale image (F1)	Pixels image	784	85.99
Knight (F2) Key of 7x7 elements	Pixels image	784	85.92
Joseph(F3) start=1; space=5.	Pixels image	784	10.00
Arnold (F4) a=1; b=5; n=1	Pixels image	784	85.99
Chaos (F5) x_0=0.1, u=4	Pixels image	784	81.24
RSA (F6)	Pixels image	784	61.15

ECC (F7)
a=-1;
b=188;
p=6563;
	Pixels image	784	35.17

In order to improve the system performance, we concatenate the grayscale image images with encrypted image, the SVM used to classify the pixels image vector from concatenate image.

Table 2. Recall on the concatenated image.

Used Image		**Dim**	**Recall (%)**
Concatenated Image (F1, F2)	Pixels image	1568	86.03
Concatenated Image (F1, F3)	Pixels image	1568	86.03
Concatenated Image (F1, F4)	Pixels image	1568	86.03
Concatenated Image (F1, F5)	Pixels image	1568	83.96
Concatenated Image (F1, F6)	Pixels image	1568	82.53
Concatenated Image (F1, F7)	Pixels image	1568	83.01

As shown in Table 2, the concatenated images are used to enhance the performance. The maximum value on the Recall produced by concatenated images be-tween Grayscale image and Knight or Joseph or Chaos outperforms all other concatenated images reporting Recall of

86.03%. It was also observed that in some cases, our proposed system could not produce desired classification results.

5 Conclusion

This work presented an effective system for isolated handwritten digit recognition that exploits encryption image techniques as features. Moreover, the proposed encryption image techniques such as Arnold is a very efficient for handwritten digit recognition which is robust. The classification of digits was performed using widely used SVM classifier. The system is evaluated using the same experimental protocol described in the Digit Recognition Competition (HDRC 2013). The results showed that our system based on Arnold technique outperforms the other encryption image technique.

General Conclusion

General Conclusion

In Image Encryption, the key is the most important thing to successful encryptionand decryption. The security of information dependson the security of the key. The traditional imageencryption algorithm cannot resist the attack of malicious key sharing and repudiation. If the key length is too large, it will be easy to lose and it will be difficult to remember the main challenge is to handle the tradeoffbetween the three requirements: privacy, accuracy and efficiency.

This work allow us to prove the efficiency of IE techniques in HDR, yet the benefit in our work is that digits need not be revealed unnecessarily as they can remain in encrypted form at all times, even during recognition process.

During this research, we carried out a series of experiments to evaluate the effectiveness of the proposed system for handwritten digits recognition on the normalized CVL Single Digit data-base. First, all handwritten digits are converted to grayscale images. Next, the encrypted image is encoded the input grayscale image. The database comprised 7,000 handwritten digits were provided as a training set and 21,780 as a test set.

Our experiments aim to study the effectiveness of the proposed system used the encryption-based encoding based on six image encryption techniques. The image encryption techniques are generated using Knight, Joseph, Chaos, Arnold, RSA and ECC from the whole image.

The results obtained by experimentation confirm the effectiveness of our approach also encouraging and promising, since the quality of the dataset is very realistic and we used different image encryption techniques.

Finally, the conclusions of this work are that the whole system needs to be efficient. The HDR system needs to be accurate, and the cryptosystems needs to be secure. We can use the learned encrypted image for HDR and gives the same performance against learned integer image.

This system corresponds the initial point for HDR based on IE, despite the results obtained, increase of performance and improvements can be considered:

- Apply the various features extraction techniques on encrypted image and compared it with original image.
- Tester with other cryptosystems.
- Improve the system by combining the classifier with other or more classifiers.
- Try the system by using another classification method.
- Tester with other databases introducing a greater number of scripters, to include more variations in writing styles, so that generalization can be more efficient.

References

References

[1]. A. GATTAL, 2011, « Segmentation automatique pour la reconnaissance numérique des chèques bancaires Algériens » ; Thèse de MAGISTER, centre Universitaire de Khanchela

[2]. Jean-Pierre « reconnaissance de l'écriture manuscrite », Département Images, ENSTParis et Guy LORETTE RISA, CNRS UPRES-A 6074, Université de Rennes 1.

[3] Noise Reduction and Pre-processing techniques in Handwritten Character Recognition using Neural Networks Magesh Kasthuri, V. Shanthi, EnathurKanchipuramPublished 2014

[4] M. Sezgin, B. Sankur, "Survey over image thresholding techniques and quantitative performance evaluation", Journal of Electronic Imaging 13 (1) (2004) 146–168.

[5] Binarization Techniques used for Grey Scale Images Puneet, Naresh Kumar Garg International Journal of Computer Applications (0975 – 8887) Volume 71– No.1, June 2013

[6] Skeletonization Algorithm for Binary Images Waleed Abu-Ain, Siti Norul Huda Sheikh Abdullah, Bilal Bataineh, Tarik Abu-Ain, Khairuddin Omar

[7] M. Zaiz Faouzi, Les Supports Vecteurs Machines (SVM) pour la reconnaissance des caractères manuscrits arabes, Université Mohamed Khider-BISKRA, pp.15 ,15/07/2010.

[8] The Role of Size Normalization on the Recognition Rate of Handwritten Numerals Chun Lei He, Ping Zhang, Jianxiong Dong, Ching Y. Suen, Tien D. Bui
Centre for Pattern Recognition and Machine Intelligence, Concordia University Montreal, Quebec, Canada

[9] HANDWRITTEN CHARACTER RECOGNITION WITH OPTIMAL ZONING USING GA Sunita B.Borse , Prof.MadhuriBhalekar , Dr. M. U. Kharat

[10] Segmentation Techniques Comparison in Image Processing R.YogamangalamB.Karthikeyan School of Computing, SASTRA University, Thanjavur, TamilNadu, India

[11]Implicit Vs Explicit based Script Segmentation and Recognition: A Performance Comparison on Benchmark Amjad Rehman, Dzulkifli Mohamad and Ghazali Sulong

[12] N. Benahmed, Optimisation de Réseaux de Neurones Pour la Reconnaissance des Chiffres Manuscrits Isolés, Sélection et Pondération des Primitives par Algorithmes Génétiques, Thèse pour l'obtention de la Maîtrise en Génie de la Pro duction Automatisée, Montréal, Mars 2002.

[13] G. Tremblay, Optimisation d'ensemble de classifieurs non paramétriques avec apprentissage par représentation partielle de l'information, Thèse de doctorat, Ecole de technologie supérieure, Université du Québec, 2004

[14] T. Thanh, Thai Hoang, Le choix de paramètres pour la reconnaissance des chiffres manuscrits, Diplôme de Magistère, University of Natural Sciences, HCMC, Vietnam.

References

[15] M. Soua, Extraction hybride et description structurelle de caractères pour une reconnaissance efficace de texte dans les documents hétérogènes scannés : Méthodes et Algorithmes parallèles, Université Paris-Est-Français, pp. 37- 38,2016.

[16] C. Bahlmann, Advanced Sequence Classification Techniques Applied to Online Handwriting Recognition. Institut for Informatic : Shaker Verlag, 2005.

[17] D. Nasreddine, Combinaison de classifieurs pour la reconnaissance hors ligne des chiffres manuscrits isolés, Université de Tébessa, pages 12–13, 2012.

[18] R. Youssef, Squelettisation d'images en niveaux de gris et applications, Université paris Descartes, École doctorale ED386 de Sciences Mathématiques de Paris Centre, 26 novembre 2015.

[19] J.P. Gastellu-Etchegorry, Acquisition et Traitement D'image Numérique, Avril 2008.

[20] S. Nemouchi, Reconnaissance de l'écriture arabe par systèmes flous, Mémoire magister, Université Badji Mokhtar, Annaba, 2010.

[21] A.K. Jain, R.P.W. Duin, J. Mao, Statistical pattern recognition : A review. IEEE Trans, on PAMI, vol. 22, no. 1, pages 4–37, 2000.

[22] B. belainine, Classification supervisée de textes courts et bruités, Université de Québec à Montréal, pages.7-10, 2017.

[23] Silva, Ribeiro, Inductive inference for large scale text classification : kernel approaches and techniques, volume 255. Springer,2009.

[24] Joachims, T. Leaming ta classify text Using suppot vector machines : Methods, theory and algorithms. Kluwer Academie Publishers, 2002.

[26] Zhu, Goldberg, Introduction to Semi-Supervised Learning. Synthesis Lectures on Artificial Intelligence and Machine Learning, 3(1), 1- 130, 2009.

[27] Abdelaali, Z. Saddam, Reconnaissance hors ligne des chiffres manuscrite isolé, Tros-Rivifieres, Université de Tébessa, pages. 12-15, 2015.

[28] N. Benamara, A. Belaid : « Une méthode stochastique pour la reconnaissance de l'écriture arabe imprimée », Forum de la recherche en informatique, Tunis, Tunisie, 1996.

[29] C.L. Liu and H. Fujisawa, Classification and Learning Methods for character recognition : advances and remaining problems, Studies in Computational Intelligence (SCI), Springer, vol. 90, pp. 139-161, 2008.

[30]. C. Chatelain. « Extraction de séquences numériques dans des documents manuscrits quelconques », Thèse de doctorat, Université de Rouen, France. , 2006 p. 196.

[31]. Y. Lei, C. S. Liu, X.Q. Ding & Q. Fu.A Recognition BasedSystem for Segmentation of Touching Handwritten Numeral Strings. IWFHR, pages 294–299, 2004.

References

[32]. P.M Lallican, C. Viarp-Gaudin and S. Knerr,. « From off-line to on-line handwriting recognition ». Proc. 7th workshop on frontiers in handwriting recognition, Amsterdam, 2000 ,pp. 303-312

[33]. Frédéric Grandidier doctorat en génie ph.d. « un nouvel algorithme de sélection de caractéristiques – application à la lecture automatique de l'écriture manuscrite »
montréal, le 24 janvier 2003

[34]. Dargenton, «Contribution à la segmentation et la reconnaissance de l'écriture manuscrite» ; Thèse de Doctorat. Institut National des Sciences Appliquées de Lyon, 174 pages. 1994
[35]. A. El-Yacoubi, R. Sabourin, M. Gilloux, and C.Y. Suen. Improved model architecture and training phase in an off-line HMM-based word recognition system. In Proc. of the 13th International Conference on Pattern Recognition, Brisbane, Australia, 1998, pages 1521–1525.

[36]. C. Chatelain. « Extraction de séquences numériques dans des documents manuscrits quelconques », Thèse de doctorat, Université de Rouen, France. , 2006 p. 196.

[37]. Burges, C. J. C., 1998. A Tutorial on support vector machines for pattern recognition, Data Mining and Knowledge Discovery (Edited by Ussama Fayyad), Vol. 2, 121-167.
[38]. C. Touzet,. « Les réseaux de neurones artificiels : introduction au connexionnisme»,150 pages, Edition EC2, Paris. 1992,pp.6-35

[39] Ernest Kussul, Tatyana Baidyk : Improved Method of Handwritten Digit Recognition, Glushkov Institute of Cybernetics, Kiev, Ukraine, 2004.

[40]. F. Menasri, «Contributions `a la reconnaissance de l'´ecriture arabe manuscrite», Thèse de doctorat, universite´ paris des cartes, juin 2008.
[41] Ming Wu Zhen Zhang, Handwritten Digit Classification using the MNIST Data Set, ResearchGate publications, 2010.

[42]. C-L. Huang, C-J. Wang, A GA-based feature selection and parameters optimization for support vector machine, Expert systems with application, vol. 31, pages 231-240, 2006.

[43]. I. Guyon, J. Weston, S. Barnhill, V. Vapnik, Gene Selection for Cancer Classification using Support Vector Machines, Machine Learning, vol. 46, no. 3, pages 389-422, 2002.

[44]. D.Abdelhakim, 2011, «La reconnaissance des chiffres manuscrits par les machines à vecteurs de support(SVMs)»; Thèse de Master, Université de Tébessa

[45] High-Speed Cryptography and Cryptanalysis / door Peter Schwabe. – Eindhoven: Technische Universiteit Eindhoven, 2011

[44] *Menezes, A.; Oorschot, P. van; Vanstone, S. (1997).* Handbook of AppliedCryptography
[46] : YAGOUB Imad Eddine, « Systèmes dynamiques discrets et chaos », université du havre, Année 2010/2011

[47] *Delfs, Hans &Knebl, Helmut (2007). "Symmetric-key encryption".* Introduction to cryptography: principles and applications. *Springer.* ISBN 9783540492436.

References

[48] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems (extended abstract). In Advances in Cryptology – Crypto '90, (eds. Alfred J. Menezes and Scott A. Vanstone),.

[49] Cipher A. Deavours and Louis Kruh. Machine Cryptography and Modern Cryptanalysis, Artech House Telecom Library. (Artech House Publishers, Norwood, MA, 1985).

[50]. Khatwani, C.; Roy, S. Security Analysis of ECC Based Authentication Protocols. In Proceedings of the 2015 International Conference on Computational Intelligence and Communication Networks (CICN), Jabalpur, India, 12–14 December 2015; pp. 1167–1172.

[51]. Burr, J. Elliptical Curve Cryptography (ECC). Available online: http://searchsecurity.techtarget.com/ definition/elliptical-curve-cryptography/

[52] Breaking an image encryption scheme based on Arnold map and Lucas series Imad El Hanouti1 · Hakim El Fadili1 · khalid Zenkouar2

[53] L. Euler. (1766). Solution d'une question curieuse que ne pariot soumise a aucune. Presented at Analyse;

[54] Hou Qibin,ZhouXiaoxu,YangXiaofan et a1.A Knight's Tour based scrambling algorithm for image encryption(in Chinese).CASIA CAIT,

[55] EmestoMordecki.On the number of Knight's Tours.2002. http://kolmogorov.croat.edu.uy/-mordeckiarticles/divisibility/

[56]. Guan P, Xue Y, Qiu Y, Sun Q (2012) A novel digital image encryptionmethodbased on onedimensionalrandomscrambling. In: IEEE 9th international conference on fuzzy systems and knowledge discovery, pp 1669–1672

[57]. Shiva Shankar S, Rengarajan A (2016) Data hiding in encrypted images using Arnold transform. ICTACT J Image Video Process 07(01):1339–1344 (2016)

[58] *Kartit, Zaid (February 2016).* "Applying Encryption Algorithms for Data Security in Cloud Storage, Kartit, et al"

[59] *Stallings, William (3 May 1990).* Cryptography and Network Security: Principles and Practice. *Prentice Hall. p. 165.* ISBN 9780138690175

[60] An introduction to cryptography and cryptanalysis Edward Schaefer Santa Clara University

[61] : Laurent Poinsot. "Introduction à la sécurité informatique".

[62] :Sandrine JULIA. "Techniques de cryptographie",2003.

[63] :Alfred J. Menezes, Paul C. van Oorschot et Scott A. Vanstone. "Handbook of Applied Cryptography ", 1996

References

[64] Amar Pandey, "Correlation Attack on Stream Cipher", International Journal of Emerging Technology and Advanced Engineering, Vol 4, Issue 4, April 2014, pp: 864-869.

[65] Bernstein D.J.et al.(2013) Factoring RSA keys from Certified Smart Cards: Coppersmith in the wild. In: Sako k., Sarkar P.(eds) Advances in Cryptology – ASIACRYPT 2013. Lecture Notes in Computer Science, Vol 8270, Springer, Berlin, Heidelberg.

[66] AbderrahmaneNitaj, Mohamed OuldDouh, "A New Attack on RSA with a Composed Decryption Exponent", International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.4, December 2013.

[67] OnurAclicmez, Cetin Kaya Koc, Jean-Pierre Seifert, "On the Power of Simple Branch Prediction Analysis".

[68]. Bos, J.; Kaihara, M.; Kleinjung, T.; Lenstra, A.K.; Montgomery, P.L. On the Security of 1024-Bit RSA and 160-Bit Elliptic Curve Cryptography; EPFL-REPORT-164549, 2009.

[69]. Garrett, K.; Talluri, S.R.; Roy, S. On vulnerability analysis of several password authentication protocols. Innov. Syst. Softw. Eng. 2015, 11, 167–176.

[70]. Higgins, K.J. Hacker's Choice: Top Six Database Attacks.

[71]. Winkler, D.C. Securing Your Password Database with Bcrypt

[71] Xiao D, Liao X, Wong K. An efficient entire chaos-based scheme for deniable authentication. Chaos, Solitons & Fractals 2005;23:1327–31.

[72] J. Fridrich J, "Secure image ciphering based on chaos", Final report for AFRL Rome, New York, 1997

[73]. O. Edward, Chaos in Dynamical Systems, Cambridge University Press, Cambridge, UK, 2003

[74] Breaking an image encryption scheme based on Arnold map and Lucas series Imad El Hanouti1 · Hakim El Fadili1 · khalid Zenkouar2

[75] I. Younas, M. Khan, A new efficient digital image encryption based on inverse left almost semi group and Lorenz chaotic system, Entropy 20 (12) (2018) 913.

[76] Vapnik V. N., The Nature of Statistical Learning Theory, Springer-Verlag, London, UK, (1995).

[77] Diem M., Fiel S., Garz A., Keglevic M., Kleber F. and Sablatnig R., ICDAR 2013 Competi-tion on Handwritten Digit Recognition (HDRC 2013), In Proc. of the 12th Int. Conference on Document Analysis and Recognition (ICDAR), pp. 1454-1459. (2013).