Proposed Model of Image Cryptography (A Designing Approach for Images Security)

Keerti Kushwaha¹, Sini Shibu²
¹M. Tech Scholar, ²Prof., CSE Dept, NIIST College Bhopal,

Abstract- Nowadays, privacy is becoming more important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Encryption is a means to achieve that privacy. It was invented for that very purpose. This paper is introduced to analysis and design a chaos based image encryption technique using the method of shuffled operation. In this new technique, a secret key of 128-bit and shuffled maps are employed. We compared the performance of new technique with the typical encryption technique in some literature. The proposed system has the advantage of larger key space; smaller iteration times, high security analysis, correlation analysis and entropy analysis will carry on.

Keyword- Security, Image, Network, Algorithm, Key

I. INTRODUCTION

Encryption is the process of scrambling a message so that only the intended recipient can read it. The actual cryptographic process is generally a complicated mathematical formulation, the more complex the more difficult to break. A key is supplied to the recipient so that they can then decipher the message. Keys for encryption algorithms are described in terms of the number of bits. The higher the number of bits the more difficult that cryptosystem would be to break. Cryptography technique is used Encryption and decryption word to implement its concept. Encryption mean systematic or step-by-step procedure called an algorithm to convert data or the plane text into unreadable form known as cipher text, its encrypted form. Decryption is also systematic or step-by-step procedure to convert cipher data or cipher text into original plane text. Encryption and Decryption normally require a string of characters called a key to encrypt or decrypt data respectively. Those who possess the key and the algorithm can encrypt the plaintext into cipher text and then decrypt the cipher text back into plaintext. So exactly does encryption work? How is data coded and decoded? This is all done using a key. A key is a long sequence of bits used by cryptography algorithms. During encryption, the algorithm alters the original data based on the key's bits to create a new encrypted message.

When the data arrives at its destination, the same or a different key is used to decode the encrypted message back into its original form. Some algorithms use the same key for encryption and decryption. The information transferred using this method is less secured because its security relies on the key being kept secret. If anyone finds out the key, they can decode the data. The algorithms use one key for encryption and one key for decryption. With this method, it's ok if the encryption key becomes public, because anyone who finds it will still not be able to decrypt the data without the decryption key. A cryptography technique is the better approach to protect information against any type of losses of the information over internet. Cryptography techniques required some sort of mathematical algorithm for encryption of data and information where only the party that shares the information could possible decrypt to use the information [11].

![Encryption and Decryption Diagram](image1.png)

Figure 1.1: Encryption and Decryption

Images represented by N x N arrays of density values can be thought of as points in an N x N-dimensional space. Points that are close to each other in that space represent images that are “similar” since the mean. There are two different approaches to classification: supervised and unsupervised. Both make use of the similarity measure introduced above, but one (supervised) classifies a set of images according to their similarity (speak: closeness in our high-dimensional space) with certain pre-given images, the other (unsupervised) classifies the images according to their intrinsic grouping or clustering within the set.
This is demonstrated schematically in the figure 2. The same set of images, represented by a set of dots, is either classified by comparing each image with a set of references (represented by fat dots), or by dividing the whole cloud of dots into clusters (indicated by dashed line) [12-13].

![Figure 1.2: Cluster Grouping of the Images](image)

For simplification of the analysis, or for the purpose of increasing the signal-to-noise ratio, classification is often carried out in a space that is of much lower dimensionality than the initial N x N space. This reduction of dimensionality is achieved by Multivariate Data Analysis [13]. There are two general groups of ‘images’: vector graphics (or line art) and bitmaps (pixel-based or ‘images’). Some of the most common file formats are [13-14]:

- **GIF** — an 8-bit (256 color), non-destructively compressed bitmap format. Mostly used for web. Have several sub-standards one of which is the animated GIF.
- **JPEG** — a very efficient (i.e. much information per byte) destructively compressed 24 bit (16 million colors) bitmap format. Widely used, especially for web and Internet (bandwidth-limited).
- **TIFF** — the standard 24 bit publication bitmap format. Compresses non-destructively with, for instance, Lempel-Ziv-Welch (LZW) compression.
- **PS** — Postscript, a standard vector format. Has numerous sub-standards and can be difficult to transport across platforms and operating systems.
- **PSD** – a dedicated Photoshop format that keeps all the information in an image including all the layers.

Encryption provides a much higher degree of security than anything else. One big area in which security is a concern is on the Internet. With the Internet holding close to an estimated 28 billion images and 2 billion web sites, it is easy to leave encrypted messages in a vast number of images as a security precaution.

These encrypted messages can be used in various different means and methods. One use of image encryption is to protect an image from it being downloaded by an anonymous user. Encrypting the image will lock the image to the designated website to prevent unauthorized downloading. For example, if a particular website has a certain image which is unique to that website and the creator does not wish other people to download that image, the creator will encrypt the image to avoid right clicking, downloading, and saving the image. Any random user can easily download a non-encrypted image, as opposed to an encrypted image, by right clicking. Image encryption also prevents bandwidth theft and unauthorized linking. With image encryption, an image can only be viewed from a registered website. Images can even be safe from the webmaster himself, without illegal scaling or resizing the image itself. The government also uses image encryption. They would use this for secure handling of intelligence data and intelligence activities. For civilians, image encryption can also be used for secure corporate communications and secure banking transactions. The medical field is another industry that uses image encryption. These encrypted images hold and store patient information. Rather than having a patient’s information in a thick folder of paperwork, the information is embedded into the patient’s x-ray image. Embedding extra information into an image using encryption is an effective method for image integrity in tele-mammography. Image encryption not only helps regular civilians but it can also be used for bad intentions. For example, terror groups such as the Hamas, Hezbollah and Al-Qaeda use un-crackable encryption to communicate about their criminal intentions without fear of outside intrusion, such as a government agency. There are two kinds of encryption, wherein, data is encrypted into an image and hidden from the public eye. Data encryption requires secret passwords and codes to view the image or hidden message. The second kind of encryption is an open key encryption which mainly prevents pretending, tampering and negation of the image itself, rather than encrypting it with data, it encrypts the image itself [13-14].

II.LITERATURE SURVEY AND PROBLEM IDENTIFICATION

The rapid growth of computer networks allowed large files, such as digital images, to be easily transmitted over the internet. Data encryption is widely used to ensure security however, most of the available encryption algorithms are used for text data. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data. For this we have study of previous research which is described below.
[2] Is devoted to implement and analyze a chaos based image encryption technique using the method of parameter modulation. The robustness of the system to opponents’ attack is enhanced by using only two rounds of iteration. The parameter modulation technique has reduced the problem of dynamical degradation. The algorithm has a large (256 bits: 128 bits for each round) key space to protect the system against Brute-force and statistical attacks. At the same time, the algorithm exhibits good encryption and security performances. This research have some parameters like Number of pixels change rate (NPCR) and unified average changing intensity (UAIC) for the encrypted image are calculated to measure the difference between the plaintext and the corresponding cipher text.

Research described in [3] has the advent of wireless communications, both inside and outside the home-office environment has led to an increased demand for effective encryption systems. The beauty of encryption technology comes out in more pronounced way when there is no absolute relation between cipher and original data and it is possible to rebuild the original image in much easier way. As chaotic systems are known to be more random and non-predictable, they can be made utilized in achieving the encryption. In [3] presented research has a chaos based encryption algorithm for images. Working of this algorithm is based on pixel scrambling where in the randomness of the chaos is made utilized to scramble the position of the data. The position of the data is scrambled in the order of randomness of the elements obtained from the chaotic map and again rearranged back to their original position in decryption process. In [4] presented research have classified various image encryption schemes and analyze them with respect to various parameters like tune ability, visual degradation, compression friendliness, format compliance, encryption ratio, speed, and cryptographic security. In [5] the encryption methods for enhancing the security of both text and multimedia contents has gained high significance in the current era of breach of security and misuse of the confidential information intercepted and misused by the unauthorized parties. Here they have proposed an enhancement to an existing algorithm proposed early in which the RGB attributes of a pixel were randomly scattered across the image. The scattering algorithm works on each of the Red, Green and Blue pixel values and breaks each of the pixel with respect to its constituent pixel attributes and scatters them across the spatial space of the image thus making it difficult to reform the original image unless each of the R G B attribute of the pixels are located and identified to which spatial coordinate they belong to.

In their enhancement, they have suggested a technique to add further confusion property in the ciphering of image by slicing the image into n number of sub images whose dimensions are kept confidential and applying the above algorithm to each of these sub images. The sub images are then shuffled so as to further add to resistance towards the deciphering attacks. In [6] images has widely used and the security of the information which images bring is becoming a serious problem. There are many shortcomings with traditional ciphers to deal with this kind of data. Because of the characteristic of chaos, the chaotic encryption becomes a good choice to encrypt image. Presented work in [6] based on logistic maps for images encryption. In this algorithm, a secret key of 80-bit and two chaotic logistic maps are employed. In [7] researches of image encryption algorithms have been increasingly based on chaotic systems, but the drawbacks of small key space and weak security in one-dimensional chaotic cryptosystems are obvious. Presented research is an image encryption scheme which employs one of the three dynamic chaotic systems (Lorenz or Chen or LU chaotic system selected based on 16-byte key) to shuffle the position of the image pixels (pixel position permutation) and uses another one of the same three chaotic maps to confuse the relationship between the cipher image and the plain-image (pixel value diffusion), thereby significantly increasing the resistance to attacks. The suggested system has the advantage of bigger key space; smaller iteration times and high security analysis such as key space analysis, statistical analysis and sensitivity analysis were carried out. In [8] encryption is used to securely transmit data in open networks. Each type of data has its own features; therefore different techniques should be used to protect confidential image data from unauthorized access. Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images. In this they introduce a block-based transformation algorithm based on the combination of image transformation and Chaos base image encryption algorithm. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm presented here, and then the transformed image was encrypted using the Chaos base algorithm. In [9] researchers have introduce a block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm presented here, and then the transformed image was encrypted using the Blowfish algorithm.
In [10] encryption is widely used to ensure security in open networks such as the internet. In this research they have presented permutation technique based on the combination of image permutation and a well known encryption algorithm called RijnDael. The original image was divided into 4 pixels × 4 pixels blocks, which were rearranged into a permuted image using a permutation process presented here, and then the generated image was encrypted using the RijnDael algorithm.

A. Problem Identification:

Many image encryption algorithms have been proposed based on chaotic signals in the recent years, but most of them suffer from the problem of key-space and dynamical degradation. From the study of previous research and other we have conclude that there are no clarifications which type of images they are using to perform image encryption and decryption procedure. We have also analyzed that there is no clarification about the configuration of machine and platform where all the experiment are calculating. From further study we have observed that Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable.

III. PROPOSED WORK

The concept of information security and the word cryptography might be intimidating and complicated. The objective of the research is to develop a tool that mediates the user and the operations to achieve information security goals. A platform independent tool with user-friendly graphical user interface, using already existing techniques and algorithms for cryptographic operations will be resulting product. People need to use the cryptographic operations in order to keep the personal sensitive information files to avert from foreigners in consideration of the security goals. The operations include bunch of algorithms to protect the attacks of foreigners to reach and read personal files that is located in personal computer or the owner would like to send somewhere.

Cryptographic operations consist of encryption and decryption techniques in computer and computer networking. In effort to keep information’s in safety such as banking account information’s or to provide file transaction without any problem such as password sharing caused such a security methods. We describe what features are in the scope of the proposed System to be developed. Proposed System will have

- Encryption / Decryption Operations
- Authenticity
- Secured Key

In most of the natural images, the values of the neighboring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors). In order to dissipate the high correlation among pixels and increase the entropy value, we propose a newly design transformation algorithm that divides the image into blocks and then shuffles their positions before it passes them to the proposed encryption algorithm. By using the correlation and entropy as a measure of security, this process results in a lower correlation and a higher entropy value when compared to using the proposed algorithm alone, and thus improving the security level of the encrypted images. There are two main keys to increase the entropy; the variable secret key of the transformation process and the variable secret key of the proposed algorithm. The variable secret key of the new design transformation process determines the constant, which is used to build the secret transformation table with a variable number of blocks. If the key is changed, another constant will be generated, and then a different secret transformation table is obtained. The variable secret key of the proposed algorithm is used to encrypt the transformed image. This encryption process decreases the mutual information among the encrypted image variables (i.e. high contrast) and thus increasing the entropy value.

A. Block Diagram of Proposed Concept:

In proposed block diagram we will select an image as an input. This image will pass through proposed algorithm. Proposed algorithm will use key to encrypt selected image, after completing process result will be display. Figure 3 is showing basic block diagram of the proposed model.
B. Proposed Model

This Paper introduce a block-based algorithm which is the combination of image transformation and Chosae base image encryption algorithm. The original image was divided into blocks, which were rearranged into a transformed image using a block based algorithm will present in future, and then the transformed image will divided into pixel blocks. This pixel block will convert into binary value. Similarly we will select a key value. This key value will transform in another sequence then it will convert in binary form. Finally key value wills XOR with Image value. Through proposed block based algorithm. Now finally we will get encrypted image.

IV. Conclusion

I will try to prove lower correlation value and higher entropy of selected images as compare existing algorithm so we can achieve higher security. For studying characteristics of image encryption, we must first analyze the implementing differences between image and text data:
1. When cipher text is produced, the decrypted text must be equal to the original text in a full lossless manner. However, this requirement is not necessary for image; the cipher image can be decrypted to an original image in some lossy manner.

2. Text data is a sequence of words, it can be encrypted directly by using block or stream ciphers. However, digital image data are represented as 2D array.

3. Since the storage space of a picture is very large, it is inefficient to encrypt or decrypt image directly. One of the best methods is to only encrypt/decrypt information that is used by image compression for reducing both its storage space and transmission time.

In general, there are three basic characteristics in the information field: privacy, integrity and availability. For privacy, an unauthorized user can not disclose a message. For integrity, an unauthorized user can not modify or corrupt a message. For availability, message is made available to authorized users faithfully. A perfect image cryptosystem is not only flexible in the security mechanism, but also has high overall secure performance, the image security requires following characteristics:

1. The encryption system should be computationally secure. It requires an extremely long time to attack, unauthorized user should not be able to read privileged image.

2. Encryption and decryption should be fast enough not to grade system performance. The algorithm for encryption and decryption must be simple enough to be done by user in personal computer.

3. The security mechanism must be as widespread as possible.

4. The security mechanism should be flexible.

5. There should not be a large expansion of encrypted image data.

REFERENCES


