International Journal of Research in Engineering and Applied Sciences (IJREAS)

Available online at http://euroasiapub.org/journals.php

Vol. 6 Issue 10, October - 2016, pp. 154~160

ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 6.573 | Thomson Reuters ID: L-5236-2015

COMPARATIVE STUDY ON EFFICIENT IMAGE ENCRYPTION TECHNIQUE

SANJIB DAS
Assistant Professor
Department of IT & Mathematics
ICFAI University Nagaland

Abstract: *The main purpose of this paper is to present an advanced system of encrypting data that combines the features of Cryptography, Visual Cryptography and Steganography in image files to transmit confidential information over an untrusted channel. These techniques individually may not provide all the security requirements, but together they create an advanced system that meet most of the security requirements.*

Keywords: *Cryptography, Visual Cryptography and Steganography.*

1. INTRODUCTION

With the growing need for Internet connectivity and maturation of the digital signal processing technology, applications of digital imaging are prevalent and are still continuously and rapidly increasing today. So, an efficient image encryption technique is always requisite, such that the users other than the sharing participant cannot recognize the image. In order to keep the confidentiality between the sender and receiver, image encryption techniques endeavour to the conversion of original image into a difficult confused image. The image encryption method should be proposed in such a way that the image changes over into a confused structure, which again changes back to justifiable structure utilizing decoding operation and therefore the message is passed on safely. This paper describes in brief the techniques of Cryptography, Steganography, and Visual Cryptography.

2. CRYPTOGRAPHY

2.1. Introduction:

Cryptography is the technique of achieving security by encoding messages to make them non-readable. **Cryptanalysis** is the techniques of decoding messages from a non-readable format back to readable format without knowing the initial process of converting the messages from readable format to non-readable format; however, the Cryptanalyst may in some case know the initial process but might not know the parameters attached to the initial process. **Cryptology** is the art and science of both Cryptography and Cryptanalysis. **Plain Text** refers to a message in its readable form i.e., not encoded. **Cipher Text** refers to a message in its non-readable form i.e., encoded. When a Plain Text message is encoded using a suitable scheme, the resultant message is a Cipher Text. **Secret key** is an input to the encryption algorithm, value independent of the Plain Text; different keys will yield different outputs. **Encryption algorithm** runs on the plaintext and the encryption key to yield the Cipher Text. **Decryption algorithm** runs on the Cipher Text and the key to produce the Plain Text.

Notation for relating the Plain Text, Cipher Text, and the keys

- C=EK(P) denotes that C is the encryption of the plain text P using the key K.
- P=DK(C) denotes that P is the decryption of the cipher text C using the key K.
- Then DK(EK(P)) = P

There are two primary techniques in which a plain text can be encoded to its corresponding cipher text: Substitution and Transposition.

2.1.1. Substitution Techniques:

In the Substitution Cipher technique, the characters of a plain text message are replaced by other characters, numbers or symbols.

Modified Ceaser cipher: Here the cipher text alphabet corresponding to the plain text alphabet is any places down the line i.e., an alphabet A in the plain text can be replaced by B, C, D … Z. Once the replacement scheme is decided, it would be constant and will be used for all other alphabets in that message. Say, if 5 is the key then, the message HELLO WORLD would be encrypted to MJQQT ATWQI. However, this substitution technique is not very secure. As the language of the plain text is English, so if a Cryptanalyst try with 25 possibilities i.e., replacing the cipher text alphabets with the one 1 place down the line, then trying with 2 places down the line and so on, he might in the maximum case try with the one 25 places down the line i.e., maximum 25 possibilities, he can decrypt the message. This kind of attempt is called Brute-force attack.

Mono-alphabetic Cipher: Rather than using a uniform scheme for all the alphabets in a given plain text message, we decide to use random substitution. This means that in a given plain text message, each A can be replaced by any other alphabet (B through Z), each B can also be replaced by any random alphabet (A or C through Z) and so on. The crucial difference being, there is no relation between the replacement of B and replacement of A. That is, if we have decided to replace each A with D, we need not necessarily replace each B with E – we can replace each B with any other character.

To put it mathematically, we can now have any permutation or combination of the 26 alphabets, which means (26 x 25 x 24 x … 2) or 4 x 1026 possibilities. This is extremely hard to crack. It might actually take years to try out these many combinations even with the most modern computers. Whatever pure substitution technique we use to encrypt data, the technique is always vulnerable to some Cryptanalytic attack.

2.1.2. Transposition Techniques:

In Transposition Techniques some sort of permutation on the plain text letters is performed. It hides the message by rearranging the letter order without altering the actual letters used.

Rail Fence Cipher: Rail fence is simplest of such technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. Plaintext = meet at the school house. To encipher this message with a rail fence of depth 2, we write the message as follows:

m e a t e c o l o s
e t t h s h o h u e

The encrypted message is:
MEATECOLOSETTHSHOHUE

Row Transposition Cipher: A more complex scheme is to write the message in a rectangle, row by row, and read the crypto text column by column, with the columns permuted according to some key. e.g., plaintext = meet at the school house.

Key:	4	3	1	2	5	6	7
Plain Text:	m	e	e	t	a	t	t
	h	e	s	c	h	o	o
	l	h	o	u	s	e	

Cipher Text: ESOTCUEEHMHLAHSTOETO

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. The transposition cipher can be made significantly more secure by performing

more than one stage of transposition. The result is more complex permutation that is not easily reconstructed.

2.2. MODERN CIPHERS:

Modern Ciphers are mostly symmetric. Three common schemes are used as the basis of these symmetric algorithms:

- Substitution.
- Permutation (Transposition).
- XOR

Substitution: Substitution involves taking one letter and replacing it with another letter. In order for this scheme to work, there must be a one-to-one mapping between the letters. For example, if the letter A is replaced with the letter W, for this scheme to work no other letter can be replaced with the letter W. If you ignored the one-to-one mapping requirement and set it up so that both A and B were replaced by W, the encryption stage would work fine. The letter A would be replaced with W, and the letter B would be replaced with W. During decryption, it would not be possible to determine accurately which letter you would use to replace W.

Permutation: With permutation, all of the letters in the plaintext message stay the same, they are just moved into different positions. Permutation is like taking five pieces from a game of Scrabble and spelling out the word HELLO. For example, assume that the plaintext message is a name, ERICCOLE. E is in the first position, R is in the second position, I is in the third position, and so on. Also assume that the key is 47153826. This key shows where each letter in the plaintext message appears in the cipher text. The encryption process uses the key to take the letter that is in the fourth position and place it in the first position. The seventh letter moves to the second position and so on, following the key. In this case the plaintext message ERICCOLE would be encrypted to CLECIERO. The reverse process can be followed to decrypt the message. During decryption we would lay the key over the cipher text, matching C to the fourth position, L to the seventh position, and so on, until we return the plaintext message.

XOR: XOR is more robust than either permutation or substitution. XOR is a mathematical operation that has a unique property: It is performed at the binary level so that it requires converting a message into its binary equivalent. If you take a plaintext message and you XOR it with a key, you would get the Cipher Text. If you XOR the Cipher Text with the same key, you will get back the original plaintext message. Common implementations of symmetric encryption include DES, Triple-DES, which is the de facto standard for symmetric encryption; and Rijndeal etc.

2.2.1. DES:

The Data Encryption Standard (DES) is one of the predominant algorithms for the encryption of electronic data. It was developed in the early 1970s at IBM and based on an earlier design by Horst Feistel.

3. STEGANOGRAPHY

3.1. Introduction:

STEGANOGRAPHY is an ancient technology that has applications even in today's modern society. It is derived from Greek words *"stegos"* meaning cover and *"graphia"* meaning writing. Steganography conceptually implies that the message to be transmitted is not visible to the normal eye. It is an art of hiding information inside information. The main objective of Steganography is mainly concerned with the protection of contents of the hidden information. *"Steganography is the art and science of writing hidden messages in such a*

way that no one apart from the intended recipient knows the existence of the message."

Some historical and modern-day examples of steganography are as follows:

- Tattoo on a Shaved Head.
- Invisible Ink: milk, lemon juice, vinegar.
- Microdot: a photograph the size of a printed period having the clarity of a type-written page.
- Null Ciphers: take the nth letter of each word in a passage in a book, magazine, etc.

3.2. Steganography methods:

The following formula provides a very generic description of the pieces of the steganography process: *Cover_medium + hidden_data + stego_key = stego_medium*

In this context, the *cover medium* is the file in which we will hide the *hidden_data*, which may also be encrypted using the *stego_key*. The resultant file is the *stego_medium* (which will, of course be the same type of file as the cover_medium). The cover_medium (and, thus, the stego_medium) are typically image or audio files. In this paper, we will focus on image files and will, therefore, refer to the **cover_image** and **stego_image**.

Before discussing how information is hidden in an image file, it is worth a fast review of how images are stored in the first place. An image file is merely a binary file containing a binary representation of the color or light intensity of each picture element (pixel) comprising the image.

Images typically use either 8-bit or 24-bit color. When using 8-bit color, there is a definition of up to 256 colours forming a palette for this image, each color denoted by an 8-bit value. A 24-bit color scheme, as the term suggests, uses 24 bits per pixel and provides a much better set of colours. In this case, each pixel is represented by three bytes, each byte representing the intensity of the three primary colours red, green, and blue (RGB), respectively. The Hypertext Mark-up Language (HTML) format for indicating colours in a Web page often uses a 24-bit format employing six hexadecimal digits, each pair representing the amount of red, blue, and green, respectively. The color orange, for example, would be displayed with red set to 100% (decimal 255, hex FF), green set to 50% (decimal 127, hex 7F), and no blue (0), so we would use "#FF7F00" in the HTML code. The size of an image file, then, is directly related to the number of pixels and the granularity of the color definition. A typical 640x480 pixel image using a palette of 256 colours would require a file about 307 KB in size (640 • 480 bytes), whereas a 1024x768 pixel high-resolution 24-bit color image would result in a 2.36 MB file (1024 • 768 • 3 bytes).

To avoid sending files of this enormous size, a number of compression schemes have been developed over time, notably Bitmap (BMP), Graphic Interchange Format (GIF), and Joint Photographic Experts Group (JPEG) file types. Not all are equally suited to steganography, however.

GIF and 8-bit BMP files employ what is known as lossless compression, a scheme that allows the software to exactly reconstruct the original image. JPEG, on the other hand, uses lossy compression, which means that the expanded image is very nearly the same as the original but not an exact duplicate. While both methods allow computers to save storage space, lossless compression is much better suited to applications where the integrity of the original information must be maintained, such as steganography. While JPEG can be used for stego applications, it is more common to embed data in GIF or BMP files.

The simplest approach to hiding data within an image file is called least significant bit (LSB) insertion. In this method, we can take the binary

representation of the hidden_data and overwrite the LSB of each byte within the cover_image. If we are using 24-bit color, the amount of change will be minimal and indiscernible to the human eye. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:

10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011

Now suppose we want to "hide" the following 9 bits of data (the hidden data is usually compressed prior to being hidden): 101101101. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in bold have been changed):

10010101 00001100 11001001
10010111 00001110 11001011
10011111 00010000 11001011

Note that we have successfully hidden 9 bits but at a cost of only changing 4, or roughly 50%, of the LSBs.

This description is meant only as a high-level overview. Similar methods can be applied to 8-bit color but the changes, as we might imagine, are more dramatic. Gray-scale images, too, are very useful for steganographic purposes. One potential problem with any of these methods is that they can be found by an adversary who is looking. In addition, there are other methods besides LSB insertion with which to insert hidden information.

Without going into any detail, it is worth mentioning steganalysis, the art of detecting and breaking steganography. One form of this analysis is to examine the color palette of a graphical image. In most images, there will be a unique binary encoding of each individual color. If the image contains hidden data, however, many colours in the palette will have duplicate binary encodings since, for all practical purposes, we can't count the LSB. If the analysis of the colour palette of a given file yields many duplicates, we might safely conclude that the file has hidden information.

But what files would you analyse? Suppose I decide to post a hidden message by hiding it in an image file that I post at an auction site on the Internet. The item I am auctioning is real so a lot of people may access the site and download the file; only a few people know that the image has special information that only they can read. And we haven't even discussed hidden data inside audio files! Indeed, the quantity of potential cover files makes steganalysis a Herculean task.

3.2.1. Other Forms of Steganography:

While much of the steganography employed today is quite high-tech, steganography itself can make use of many low-tech methods. The goal of stego is merely to hide the presence of a message.

One common, almost obvious, form of steganography is called a null cipher. In this type of stego, the hidden message is formed by taking the first (or other fixed) letter of each word in the cover message.

Another form of steganography uses a template (e.g., a piece of paper with holes cut in it) or a set of preselected locations on the page to hide a message. In this case, obviously, the sender and receiver must use the same template or rules.

There are other alternatives to the template method such as:

1. Pinpricks in maps to use as an overlay for relevant letters in messages.
2. Deliberate misspelling to mark words in the message.
3. Use of small changes in spacing to indicate significant letters or words in a hidden message.
4. Use of a slightly different font in a typeset message to indicate the hidden letters (e.g., the difference between

Courier and Courier New is barely noticeable unless you are looking for it).

4. VISUAL CRYPTOGRAPHY

4.1. Introduction:

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption can be performed by humans, without computers i.e., reconstructed visually.

4.2. Visual Cryptography Scheme:

- Scheme that uses Cryptography that considers the problem of secure communication.
- Scheme that uses Visual Cryptography that allows decryption without using any computation or knowledge about Cryptography.
- Schemes that conceals the existence of secret message.

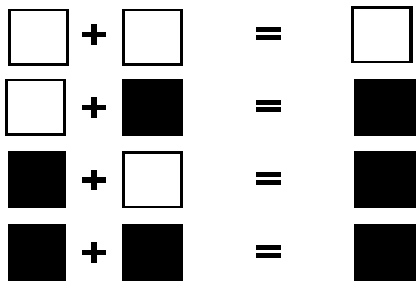
4.2.1. Advantages:

- An advantage of Visual Cryptography Schemes is the property that VCS decoding relies purely on human visual system.
- Visual Cryptography is used with short messages, therefore giving the cryptanalyst little to work with.
- Since Visual Cryptography uses short message, public keys can be encrypted using this method.
- Visual Cryptography has proved that security can be attained with even simple encryption schemes.

An application of Visual Cryptography is VCRYPT that provides secure transmission of Data via Email or FTP, maintains authenticity of the document and is also easy and inexpensive to decrypt.

4.3. Visual Secret Sharing:

- Any share by itself does not provide any information, but together they reveal the secret.
- Shares are images printed on transparencies. The secret is reconstructed by the eye not a computer.
- Decryption by superimposing the proper transparencies.
- Bits of the shares are combined as xi OR yi



Since ({0,1}, OR) is not a group we need to introduce redundancy.

4.3.1. Sharing Matrix representation: S = [S_{ij}] a boolen matrix with:

- a row for each share, a column for each subpixels.
- S_{ij} = 1 iff the j^{th} subpixel of the i^{th} share is dark.
- one set of matrices for "0" and one for "1" (or one for each grey-level in secret image).
- "normally" each set is the column permutations of base matrix.
- for each pixel, choose a random matrix in the corresponding set ("normally" with equal probabilities).

Properties of Sharing Matrices:

For Contrast: sum of the sum of rows for shares in a decrypting group should be bigger for darker pixels.

For Secrecy: sums of rows in any non-decrypting group should have same probability distribution for the number of 1's in S_0 and in S_1.

5. CONCLUSION

In this paper various image encryption algorithms are discussed. Some algorithms are working on R.G.B color system and others are working on grayscale image. These encryption algorithms are studied well under the different parameters to promote the performance of the encryption methods as well as to ensure the security proceedings. Overall, all the techniques are useful for real-time encryption. All the techniques are unique in its own way, which might be suitable for different applications.

References:

[1] Yaobin Mao and Guanrong Chen "A Novel Fast Image Encryption Scheme Based on 3d Chaotic Baker Maps" International Journal of Bifurcation and Chaos, Vol. 14, No. 10 (2004) 3613–3624.

[2] Alireza Jolfaei, Abdolrasoul Mirghadri "An Image Encryption Approach Using Chaos and Stream Cipher" Journal of Theoretical and Applied Information Technology 2010.

[3] Musheer Ahmad and M. Shamsher Alam "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping" International Journal on Computer Science and Engineering, Vol.2 (1), 2009, 46-50.

[4] Xin Ma, Chong Fu, Wei-min Lei, Shuo Li "A Novel Chaos-based Image Encryption Scheme with an Improved Permutation Process" International Journal of Advancements in Computing Technology Volume 3, Number 5, June 2011.

[5] Zhang, G. J., Liu, Q. "A Novel Image Encryption Method Based on Total Shuffling scheme" Optics Communications, 284, pp. 2775--2780 (2011).

[6] Bourbakis N, Alexopoulos C (1992) Picture data encryption using scan patterns. Pattern Recognition 25(6):567 – 581

[7] C.E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technology J, vol.28, 1949, pp .656–715.

[8] M. Henon, "A Two-Dimensional Mapping with a Strange Attractor," Communication in Mathematical physics, vol. 50, 1976, pp. 69–77.

[9] Ljupco Kocarev, Chaos-Based Cryptography: A Brief Overview.

[10] Xingyuan Wangn; LinTeng,XueQin, A novel colour image encryption algorithm based on chaos, Signal Processing 92 (2012) 1101–1108, 2011 Elsevier.

[11] S. S. Askar; A. A. Karawia; Ahmad Alshamrani, Image Encryption Algorithm Based on Chaotic Economic Model Volume 2015, Article ID341729,10pageshttp://dx.doi.org/10.1155/2015/341729.

[12] A Mitra; Y. V. Subba Rao; S. R. M. Prasanna,A New Image Encryption Approach using Combinational Permutation Techniques, International Journal of Electrical and Computer Engineering 1:2 2006.

[13] H. H. Nien; W. T. Huang; C. M. Hung, Hybrid Image Encryption Using Multi-Chaos-System, 2009 IEEE.

[14] Chen Wei-bin; Zhang Xin, Image Encryption Algorithm Based on Henon Chaotic System, 2009 IEEE.

[15] Tiegang Gao; Zengqiang Chen, Image encryption based on a new total shuffling algorithm, Elsevear.