An Innovative Approach for Secret Hiding Based on Visual Cryptography Scheme

Ravi Kumar Goel[1], Mr. Jujhar Singh[2]

[1]Research Scholar, Department of Computer Science, GITM, Karnal, Haryana, India

[2]Assistant Professor, Department of Computer Science, GITM, Karnal, Haryana, India

Abstract- Cryptography is the art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. The message can be deciphered (or decrypted) into plain text only by those who possess a secret key. Encrypted messages sometimes can be broken by cryptanalysis which is also called code-breaking, although modern techniques are virtually unbreakable. Electronic security is becoming increasingly important as the Internet and other forms of electronic communication become more prevalent. Steganography derives from the Greek word steganos, meaning covered or secret, and graphy (writing or drawing). Steganography is a technology where modern data compression, information theory, spread spectrum, and cryptography technologies are brought together to satisfy the need for privacy on the Internet. This paper is an attempt to analyze the various techniques used in steganography and to identify areas in which this technique can be applied, so that the human race can be benefited at large. This Proposed work will help us to hide the secret code in the images. So, this scheme can possibly be modified to hide two independent coloured secret images into n meaningful coloured cover images. The recovery process of both secret images should remain lossless while using the same expansion factor.

Keywords – *Cryptography, Steganography, Encryption, Decryption, Visual Cryptography, Cryptanalysis*

1. INTRODUCTION

Cryptography (from Greek krypto's, "hidden", and gr'aphein, "to write") is, traditionally, the study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge — the art of encryption. In the past, cryptography helped ensure secrecy in important communications, such as those of spies, military leaders, and diplomats. In recent decades, the field of cryptography has expanded its remit in two ways. Firstly, it provides mechanisms for more than just keeping secrets : schemes like digital signatures and digital cash, for example. Secondly, cryptography has come to be in widespread use by many civilians who do not have extraordinary needs for concealment, although typically it is transparently built into the infrastructure for computing and telecommunications, and users are not aware of it. Cryptography has had a long and colourful history. Generally speaking the earliest forms of secret writing required only pen and paper, and are now collectively termed classical cryptography.

Cryptographic systems are characterized as:

The type of operations used to transforming plaintext to cipher text: All the encryption algorithms are based on substitution in which one element is replaced for another, and transposition in which the order of the elements is rearranged. Most systems involve multiple stages of substitutions and transpositions.

The number of key used: In symmetric encryption, only one key is used for encryption and decryption. It is referred as secret key, single key or conventional encryption. In asymmetric encryption, two keys are used. It is also referred as two key, or public key encryption.

Ways of processing the plaintext: There are two ways to process the plaintext: viz. Block cipher, and stream cipher. In the clock cipher, the input plaintext is divided into block and each block is processed at a time. The result of block cipher is one block for each block of input plaintext. In stream cipher, we process the input elements continuously one by one. The result of steam cipher is one element for each element of input plaintext.

In visual cryptography [2] or visual secret sharing (vss), the original input image is shared between a set of participants P by a dealer (secret image holder). Based on the sharing policy, only qualified subsets of participants can recover the original input image.

Two important factors that used to determine the efficiency of any visual cryptography scheme, namely:

1) The quality of the reconstructed image

2) The pixel expansion (m).

Any loss of information during the reconstruction phase leads to reduction in the quality of the recovered image. On the other hand pixel expansion refers to the number of sub pixels in the generated shares that represents a pixel of the original input image. For bandwidth constrained communication channels it is desirable to keep m as small as possible. For colour images, reducing pixel expansion is of paramount importance since they occupy more space and consume more bandwidth compared to grayscale and binary images. Most of the previous works in this area try to optimize pixel expansion or obtain perfect reconstruction. In Visual Cryptography schemes (VCS) the traditional stacking operation of sub pixels and rows interrelations is modified. This new technique does not require transparencies stacking and hence, it is more convenient to use in real applications. However, it requires the use and storage of a Colour Index Table (CIT) in order to lossless recover the secret image. CIT requires space for storage and time to look up the table. Also, if number of colours c increases in the secret image, CIT becomes bigger and the pixel expansion factor becomes significant which results in severe loss of resolution in the camouflage images. Ours is an advanced scheme for hiding a coloured image into multiple images that does not require a CIT. This technique achieves a lossless recovery of the secret image but the generated shares (camouflage images) contain excessive noise. Visual cryptography is a new cryptographic scheme where the cipher text is decoded by the human visual system. Hence, there is no need to any complex cryptographic computation for decryption. The idea is to hide a secret message (text, handwriting, picture, etc…) in different images called shares or cover images. When the shares (transparencies) are stacked together in order to align the sub pixels, the secret message can be recovered.

RSA Algorithm

RSA is one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent system in 1973, but it wasn't declassified until 1997. A user of RSA creates and then publishes a public key based on the two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Breaking RSA encryption is known as the RSA problem. It is an open question whether it is as hard as the factoring problem. The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring large numbers and the RSA problem. Full decryption of an RSA cipher text is thought to be infeasible on the assumption that both of these problems are hard, i.e., no efficient algorithm exists for solving them. Providing security against partial decryption may require the addition of a secure scheme. The RSA problem is defined as the task of taking eth roots modulo a composite n: recovering a value m such that c ≡ me (mod n), where (n, e) is an RSA public key and c is an RSA cipher text.

2. Visual Cryptography

Visual cryptography [9] schemes based on access structures and graph theory are also considered. In this type of visual cryptography schemes, some definite sets of qualified participants from a general set P of participants can be chosen. The qualified subsets are the only ones that can reconstruct the secret information. Visual Cryptography is a graphical form of information concealing. It can be seen as a cryptographic primitive, since it offers methods and technologies for building more complex information security systems. The dealer chooses a secret message that can be written text, a picture, a scheme, a spreadsheet calculation etc. and splits it in two "shadow images" called shares. Every participant to the scheme will receive a separate share printed onto a transparency. In the decryption process, the participants only have to carefully superimpose their shares and the secret will be visually revealed. Such a scheme will be called a two–out–of–two visual cryptography scheme.

A visual cryptography scheme is a secret sharing scheme to encode a secret image SI in such a way that any qualified subset of participants can "visually" recover the secret image, while forbidden subsets have no information on SI. A "visual" recovery consists of Xeroxing the shares, which are shadow images, onto transparencies and stacking them one on the top of the others. The participants in a qualified subset will be able to see the secret image without any knowledge of cryptography and without performing any cryptographic computation. Visual cryptography is a powerful tool for teaching cryptography to general audience. Applications have also been proposed to realize authentication, identification schemes and, recently, e voting schemes.

Visual Cryptography in Biometric Applications

A biometric authentication system operates by acquiring raw biometric data from a subject (e.g., face image), extracting a feature set from the data (e.g., Eigen-coefficients), and comparing the feature set against the templates stored in a database in order to identify the subject or to verify for a claimed identity. The template of a person in the database is generated during enrolment and is often stored along with the original raw data. Protection of biometric data is gaining importance because its uniqueness and digital watermarking techniques are used to protect the biometric data from either accidental or intentional attacks. Here introduces a novel secured authentication method using wavelet decomposition and Visual Cryptography to hide an iris image. In this technique, iris image is embedded in cover image and then using wavelet transforms this output image is decomposed into four shares. These four shares are compressed at sender site. At receiver side, to obtain original iris image inverse DWT is obtained and finally bit matching procedure has been applied. The result shows that Steganography[6] and Visual cryptography implementation on biometrics, secures Iris and related textual information from getting identity forged.

Visual cryptography[8] technique is used to make the data secure. Here the original data is divided into a number of shares which are sent through different communication channels from sender to receiver. Therefore the intruder has less chance to get the whole information. But still it is not so secured. This can be made more secure by introducing a symmetric key for both encryption and decryption process. Using the key, the image[1] is first encrypted then divided into a number of shares. If the intruder gets k number of shares s/he cannot be able to decrypt it if the key is not known to his/her. For key, a combination of character or number can be used. The change of higher bits make the image more blur, so the key can be applied on the higher bits of each pixels.

3. Proposed Algorithm

The proposed approach uses meaningful shares (cover images) to hide the coloured secret image and the recovery process is lossless. The scheme defines a new stacking operation (XOR) and requires a sequence of random bits to be generated for each pixel. This scheme can be generalized to an n out of n approach.

Methodology

Assume that a gray image with 256 colours constitute a secret to be hidden. Each colour can be represented as an 8-bit binary vector. The main idea is to expand each coloured pixel into m sub pixels and embed them into n shares. This scheme uses m=9 as an expansion factor. The resulting structure of a pixel can be represented by an nx9 Boolean matrix S= [Sij] where (1≤ i ≤ n, 1≤ j≤ 9) and Sij =1, if and only if, the jth sub pixel in the ith share has a non-white colour. To recover the colour of the original secret pixel, an “XOR” operation on the stacked rows of the n shares is performed.

Recovering Algorithm

In order to recover the secret image in a 2 out of 2 scheme, both camouflage images O1’, O2’ as well as the string of random bits R are required for the recovery process the camouflage images are t time bigger than IHL due to the expansion factor of subpixels.

Steps of the Algorithm

Extract the first 3x3 blocks $V^1{}_r$ and $V^2{}_r$ from both camouflage images O^1’and O^2’, respectively.

Re-arrange $V^1{}_r$ and $V^2{}_r$ in a 2x9 matrix format S_r.

Select the first random bit r_p corresponding to the first encrypted pixel.

Input S_r and r_p to the function corresponding to equation (1).

Recover k_p, the first pixel in I_{HL}.

Repeat for all 3x3 blocks in O^1'and O^2

Improved image generation scheme

Algorithm to generate better quality camouflage images is given. Most of the modifications are applied to the sub pixel expansion block described in the next section.

Hiding Algorithm

Before sub pixel expansion, add one to all pixels in the cover images and limit their maximum value to 255. This ensures that no "0" valued pixels exist in the images. When the images are expanded, replace all the 0's in S0, S1 by values corresponding to k1-1 in B1 and k2-1 in B2 (Figure 1) instead of leaving them transparent. Also, adjust all pixel values to be between 0-255

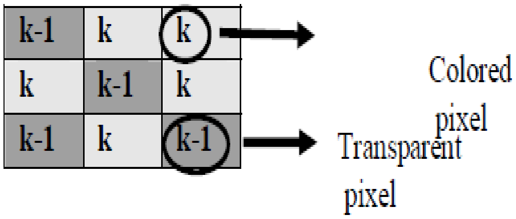

Figure 1: Improved block subpixel expansion technique

Decryption algorithm

To recover the secret image, both camouflage images O^{1}', O^{2}' and the string of random bits R are required.

Steps of the Algorithm

Take all regions of size txt in the camouflage images.

Re-structure the square matrices as 1xm vectors.

Scan through the 9 subpixels in the vector and note the coordinates of the k1 and the k1-1 colours previously encrypted.

Count the number of k and k-1 pixels in the processed vector, denoted as count k-1, count k, respectively.

If count k-1 < count k , the transparent pixel is colour k-1, otherwise, set it to k.

Use the k1 and k2 colours to find the secret pixel using the F(.,.) function and the random number previously transmitted.

4. Results

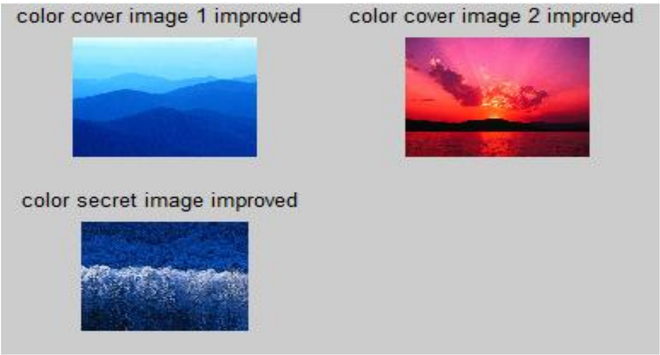
color cover image 1 improved
color cover image 2 improved
color secret image improved

Figure 2: Displaying input images in RGB colour space

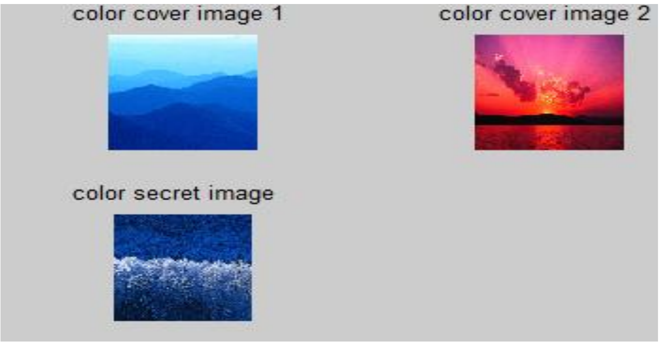

Figure 3: Resizing the images

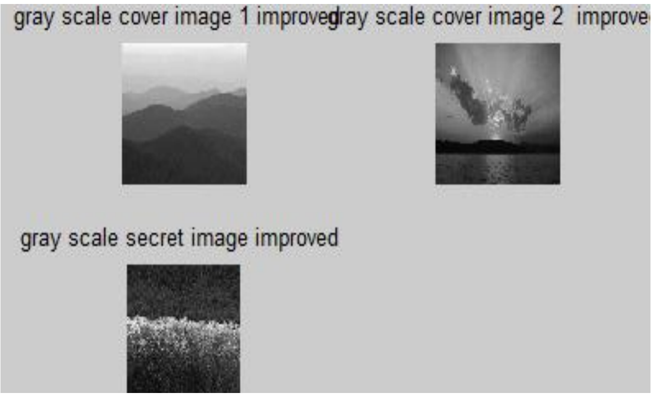
gray scale cover image 1 improved
gray scale cover image 2 improve
gray scale secret image improved

Figure 4: Displaying gray scale images

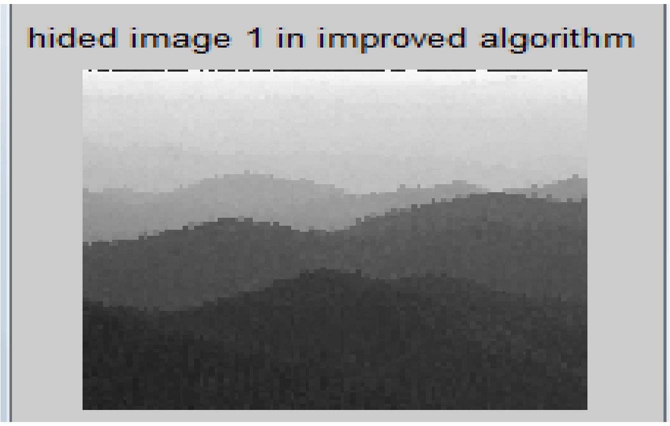

Figure 5: After using algorithm the hided image obtain by first cover image

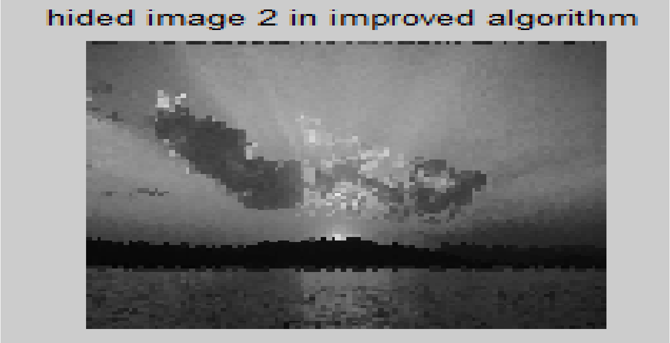

Figure 6: After using algorithm the hided image obtain by second cover image

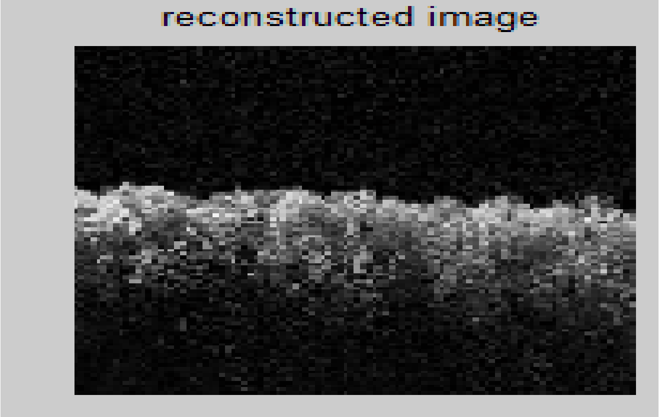

Figure 7 : Reconstructed image obtained from two hided images in Gray Scale

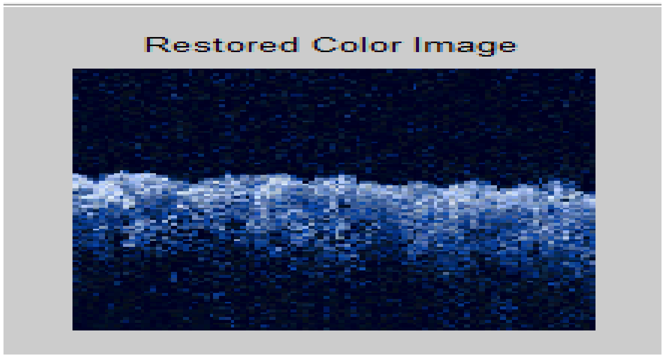

Figure 8: Restored Colour image from reconstructed gray scale image

A secret image is hidden in two cover images. The reconstruction of hidden image is done. The decryption is done using very less cryptographic computation. A 100X100 secret image is hidden into two 100X100 cover image.

5. CONCLUSION

A new technique based on algorithm to hide a colour secret image into multiple coloured images is implemented. The generated camouflage images contain less noise compared to the ones previously obtained using the original Chang's embedding algorithm. This results in a considerable improvement in the signal to noise ratio of the camouflage images by producing images with similar quality to the originals. An improvement in signal to noise ratio of 9.3 dB and 19.97 dB were obtained for the initial camouflage images used for hiding the secret image. This developed method does not require any additional cryptographic computations and achieves a lossless recovery of the secret image. In addition, the camouflage images obtained using the modified algorithm look less susceptible of containing a secret message than the ones obtained using the original method.

6. Future Scope

This scheme can possibly be modified to hide two independent coloured secret images into n meaningful coloured cover images. The recovery process of both secret images should remain lossless while using the same expansion factor as described in this thesis. In today's world the protection of sensitive data is one of the most critical concerns for organizations and their customers. This, coupled with growing regulatory pressures, is forcing businesses to protect the integrity, privacy and security of critical information. As a result cryptography is emerging as the foundation for enterprise data security and compliance, and quickly becoming the foundation of security best practice. Cryptography, once seen as a specialized, esoteric discipline of information security, is finally coming of age.

No one would argue that cryptography and encryption are new technologies. It was true decades ago and it is still true today – encryption is the most reliable way to secure data. National security agencies and major financial institutions have long protected their sensitive data using cryptography and encryption. Today the use of encryption is growing rapidly, being deployed in a much wider set of industry sectors and across an increasing range of applications and platforms.

References

[1] Chang, C. C. and Yu. T. X.,"Sharing a Secret Gray Image in Multiple Images", in the Proceedings of International Symposium on Cyber Worlds: Theories and Practice, Tokyo, Japan, Nov. 2002, pp.230-237.

[2] M. Naor and A. Shamir, Visual cryptography. Advances in Cryptology EUROCRYPT '94. Lecture Notes in Computer Science, (950):1–12, 1995

[3] C. Chang, C. Tsai, and T. Chen, A new scheme for sharing secret colour images in computer network. In the Proceedings of International Conference on Parallel and Distributed Systems, pages 21–27, July 2000.

[4] E. Verheul and H. V. Tilborg., Constructions and properties of k out of n visual secret sharing schemes. Designs, Codes and Cryptography, 11(2):179–196, 1997.

[5] R. Hwang and C. Chang. Some secret sharing schemes and their applications. Ph.D. dissertation of the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan, 1998.

[6] C.P. Sumathi,T.Santanam and G.Umamaheswari, "A study of steganography techniques,"study the stegnography methods, Vol.4, No.6, December 2013.

[7] L.N. Pandey and Dr. Bhatele,"A comparative survey,"Visual Cryptography Schemes, Volume 1, Issue 2, July 2013 ISSN: 2320-9984 (Online)

[8] B. Madhuravani,Dr. P. Bhaskara Reddy,P. LalithSamanthReddy,"Study the detail survey of steganography", Issue 4 volume 2, March-April 2014 ISSN 2249-9954.

[9] Sonal Wange ,"A review of Visual Cryptography to secure biometric database", Volume 3, Issue 11, November 2013 ISSN: 2277 128X

[10] L.N. Pandey and Neeraj shukla,"Visual cryptography schemes using compressed random shares", Volume 1, Issue 4, September 2013 ISSN: 2321-7782