A New Approach towards Least Significant Bits Information Hiding by Secure Data Splitting & Embedding Algorithm

Ankur Chaudhary[1], Wajahat GH MOHD[2]
JB Institute of Technology
er.ankurc5@gmail.com[1], wajahatiust040@gmail.com[3]

Abstract—An improved Least Significant Bits (LSB) information hiding is proposed according to Secure Data Splitting Algorithm and Data Embedding Algorithm and based on this, quality will be managed by PSNR (Peak Signal to Noise Ratio) and MSE (Mean Squared Error) control monochromic images. So mainly what we are going to do is that an effort has been made to propose and implement a new stegano graphic technique for images by modifying existing algorithms. This technique uses LSB steganography as our basis and disperses a secret message over the entire image taken by us to ensure that the secret message cannot be get from the image. When we compare with other existing algorithms, we can easily prove that the difficulty of decoding the proposed algorithm is high.

Keywords- LSB Algorithm, Visual cryptography, Stegno image, Splitting and Embedding Algorithm.

1 INTRODUCTION

Among different kinds of the carrier media, digital images are the most popularly used data on the Internet. A host image used to hide the secret data is called the cover image or the carrier image. When the secret data has got embedded into the cover image, the resultant image is called the stego image. Good stego image quality can avoid arousing suspicion during data transmission. In terms of the processing domain, image hiding schemes can be classified as either spatial-domain or frequency-domain image hiding schemes. Methods in the spatial domain embed secret data into cover pixels directly.

One simple method is least significant bits (LSB) substitution. Methods in the frequency-domain transform each cover pixel from the spatial domain to the frequency domain. Then, the secret data are embedded into the transformed coefficients. In general, methods in the spatial domain get higher hiding capacities but low robustness, and vice versa.

Previous image hiding schemes embed the secret into the digital image, and only people with the correct key can extract and decode the secret from the embedding image. If more than one person wants to share the secret, well, previous image hiding schemes cannot do anything about it.

1.1 Research Motivation

Security has become an inseparable issue as information technology is ruling the world now. Cryptography is the study of mathematical techniques related aspects of Information Security such as confidentiality, data security, entity authentication and data origin authentication, but it is not the only means of providing information security, rather one of the techniques. Visual cryptography is a new technique which provides information security which uses simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. This technique allows Visual information (pictures, text, etc) to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms. This technique encrypts a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are usually presented in transparencies. In this paper we provide an overview of the emerging Visual Cryptography (VC) and related security research work done in this area.

In recent years digital image-based steganography has established itself as an important discipline in signal processing. That is due in part to the strong interest from the research community. Unfortunately, given the high volume of the introduced techniques, the literature lacks a comprehensive review of these evolving methods.

All of the existing methods of steganography focus on the embedding strategy and give no consideration to the pre-processing stages, such as encryption, as they depend heavily on the conventional encryption algorithms which obviously are not tailored to steganography applications where flexibility, robustness and security are required. Andreas Westfield, a steganography scholar at Dresden University, called upon researchers in the field to analyze the interaction between steganography and encryption, the crypto-stego interface.

Many of the current methods take for granted that resilience to noise, double compression, and other image processing manipulations are not required in the steganography context. As such, in the warden passive attack scenario their hidden data will be destroyed or will not be retrievable.

Adaptive steganography aimed at identifying textural or quasi-textural areas for embedding the secret data runs into a few problems at the decoder side since its classification algorithms are not salient. In this thesis, skin-tone areas are the preferred choice for texture detection since the detection algorithm is robust and unique.

Moreover, skin-tone areas always exhibit chrominance values residing along middle range, therefore, the problem of underflow or overflow is overcome automatically. In the process of searching for a good skin-tone detection algorithm, the various available techniques are proven to either be slow in execution and/or come with intolerable false alarms. Often, these algorithms neglect the fact that luminance can help improve their performance.

1.2 Research Objective

1 Study the Data Hiding techniques by using Visual Cryptography techniques and their Noise and how to improve PSNR.

2 Develop the basic procedure for Least Significant Bit Algorithm (LSB).

3 Analyze the performance of proposed methods in terms of Visual Cryptography robustness of the steago image using PSNR calculations.

4 Implement the LSB method to analysis of PSNR.

5 Algorithm results based on LSB method using MAT Lab Simulation.

1.3 Research Contribution

This research work focuses on the tradeoff analysis of data hiding by using visual cryptography for gray-scale images using Least Significant Bit (LSB) and design, implement and improve PSNR using Least Significant Bit (LSB) by proposing methods of embedding and extracting the digital image. This consists of secret image embedding, attacks and secure data extraction. The performances of proposed methods will evaluate in terms of quietness and robustness. Experimental results of the proposed methods' performance will analyze using Peak Signal to Noise Ratio (PSNR) calculations.

There are a number of algorithms or transformations are used in Visual Cryptography for robustness, but we will use the LSB method and calculate the PSNR for robustness.

1.4 Dissertation Organization

Chapter 2, it discussed the background information and history of Visual Cryptography and Steganography and also describe the Peak Signal to noise Ratio.

In chapter 3, this gives the complete details of Least Significant Bit (LSB) method for embedding the secure data into cover Image.

In Chapter 4, these describe the secure data Splitting and Embedding Algorithms.

In chapter 5, this chapter gives the information about the simulation as well as results related to the subject of analysis.

In chapter 6, we explained the conclusion of the work which is analyzed in this thesis and also some possible future works are suggested to extend this research for academic works as well.

2 CRYPTOGRAPHY

Cryptography is the science of writing in secret code the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

Cryptography is the art of achieving security by encoding messages to make them non-readable. It is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication.

Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

Cryptography is study of mathematical technique to provide the methods for information security. It provides such services like authentication, data security, and confidentiality. Visual cryptography is one of the techniques used in modern world to maintain the secret massage transmission.

Visual cryptography is based on the images and is obtained by sending pixel information. Visual

Cryptography schemes depend on sub-pixels and its complexity, computation, reliability, etc. The image consists of black and white, grayscale color images. Visual cryptography uses participates to send secret information.

2.1 Visual Cryptography

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers). The first visual cryptographic technique was developed by MoniNaor and Adi Shamir in 1994. It involved breaking up the image into n shares so that only someone with all

n shares could decrypt the image by overlaying each of the shares over each other. Practically, this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other. In their technique n-1 shares reveals no information about the original image.

Basic visual cryptography is based on breaking of pixels into some sub pixels or we can say expansion of pixels. Fig 2 shows two approaches for (2, 2) –Threshold VCS. In this particular figure first approach shows that each pixel is broken into two sub pixels. Let B shows black pixel and T shows Transparent (White) pixel. Each share will be taken into different transparencies. When we place both transparencies on top of each other we get following combinations, for black pixel BT+TB=BB or TB+BT=BB and for white pixel BT+BT=BT or

TB+TB=TB. Similarly second approach is given where each pixel is broken into four sub pixels. We can achieve 4C2 =6 different cases for this approach.

Working of Visual Cryptography

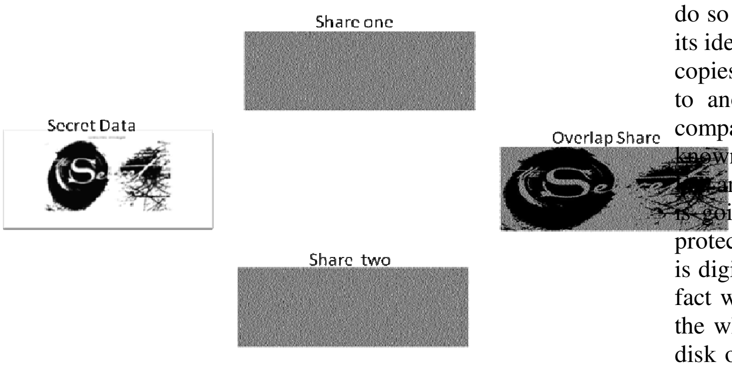

Figure2.2 Working of Visual Cryptography

Visual cryptography technique allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system. This technique used to encrypt an image into shares such that stacking a sufficient number of shares reveals the secret images. In visual cryptography there are different technique like sub pixel, error diffusion, Boolean operation etc

Visual Cryptography provides information security using simple algorithm. This technique allows visual information to be encrypted using some cryptographic schemes and their decryption can be performed by the human visual systems without any complex cryptographic algorithms. It encrypts the secret image into shares and the stacking of sufficient number of shares reveals the original image. Shares are usually represented in transparencies.

3 INFORMATION HIDING

While all the above mentioned cryptosystems have solved the problem of protecting privacy of information content they have not protected the anonymity of its sender and receiver. In fact when data is encrypt edits random nature looks strange enough to make it stand apart from normal communications. Thus it perfectly reveals that an encrypted communication is taking place between the two parties. In some other cases just leaking the existence of communication is enough to render the system unusable For example when the drug criminals hear the encrypted communication of the police over cellular phones in the region they will immediately stop and escape to other regions. In such cases it is clear that the police want its communication to be hidden from the drug criminals. In another case when some vehicle starts its encrypted communication its exact location can be immediately calculated with two directional radars In network security the corresponding problem is called the tracanalysis problem. Information hiding is not only used in military and police contexts but it is also needed in the commercial world. A company needs to protect its vital financial documents. It can do so for example by programming the word processor to hide its identification number in each electronic copy as well as hard copies of every document. Later if a document is found leaked to another place i.e in the news media or at a competing company the leakage can be traced back to its originator This is known as the tracing traitors problem.

As an abuse of this see e.g. as digital audio and video content is going to be more dominant over the analog one copyright protection is also a more serious problem When the information is digitalized the price of making a copy goes almost to zero In fact with a computer and a few commands everyone can copy the whole content of a CD or DVD to a magnetic tape a hard disk or to another CD or DVD In the case of the Internet the Web it is even easier Without any high tech skill anyone can choose to download and save an image or music clip with only a mouse click away.

Several solutions have been proposed to prevent this but few if any seems to protect the copyright perfectly while still maintaining the quality of the original document Companies such as IBM, Sony, Microsoft and AT&T have started collaborating together in seeking ways to hide copyright information into music and video. This copyright information can later be checked by viewing or copying devices. Thus an important requirement for the hiding operation is that it must retain the high quality of the media at least in the perception of the viewers and listeners.

There is another application of information hiding In many countries where the use of cryptography are conditional or controlled individual users still want to protect their privacy but would not want to be noticed In such cases information hiding gives a satisfactory answer to the problem. It hides information to be sent into normal communication. If the hiding is perfect then even the existence of the secret communication is un detect able thus privacy of the communication is maximally protected. A covert channel by its definition is hiding information into other unusual channels that were not designed to be communication channel. For instance current CPU or disk load etc can be used as a mean of communication among users or processes in a computer system.

3.1 Threshold VCS

Visual cryptography was first introduced by Na or and Shamir in 1994. In their paper, they address the idea of visual cryptography for threshold structures. They assume that the image is composed of black and white pixels, and each pixel is encrypted separately. Each pixel of the image appears in the n shares distributed to the participants. It is divided into m sub pixels, either black or white, which are sufficiently small and close that the eye averages them to some shade of grey. We can represent this with an n × m matrix: S[i, j] = 1 if and only if the jth sub pixel in the ith share is black. When the shares are combined, the perceived grey level is proportional to the number of ones in the Boolean OR of the m-vectors

representing the shares of each participant. The black and white areas of the image are determined by a rule of contrast based on three variables: a threshold value, a relative difference, and the number of sub pixels (referred to as the pixel expansion).
We use:

- t to denote the threshold value;
- α to denote the relative difference;
- m to denote the pixel expansion.

The threshold value is a numeric value for the point at which black areas are distinct from white. The value α · m is the contrast, which we want to be as large as possible. We require that α · m ≥1 to ensure that the black and white areas will be distinguishable.

We give the following definition of a threshold VCS, by Na or and Shamir .The phrasing is taken directly from Atienese, Blundo, De Santis, and Stinson .We use OR V to denote the boolean operation OR of a set of vectors with result V. The Hamming weight w (V) is the sum of the elements in a boolean vector V (alternatively, the number of 1's in V).

We can achieve this by using one of following access structure schemes.

1. **(2, 2) – Threshold VCS**: This is a simplest threshold scheme that takes a secret image and encrypts it into two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.
2. **(2, n) – Threshold VCS:** This scheme encrypts the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.
3. **(n, n) – Threshold VCS:** This scheme encrypts the secret image into n shares such that only when all n of the shares are combined will the secret image be revealed. The user will be prompted for n, the number of participants.
4. **(k, n) – Threshold VCS:** This scheme encrypts the secret image into n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted for k, the threshold, and n, the number of participants.

The Color Visual Cryptography is a visual sharing scheme, where the original color image is transformed into three color components red, green and blue. These three components are converted into halftone images and when overlapping these shares, three color components are obtained which reveals meaningful visual information.

A visual cryptography scheme can then be constructed by picking shares in the following manner:-If the pixel of the original binary image is white, randomly pick the same pattern 0 off our pixels for both shares. It is important to pick the patterns randomly in order to make the pattern random. If the pixel of the original image is black, pick a complementary pair of patterns, i.e., the patterns from the same column.

4 PROPOSED ALGORITHM

Problem definition: Given a cover image c and the image to be embedded (payload) h; the objective is,
(i) To embed the payload in the cover image by replacing LSB bits of cover image by the image of the payload. The combined image is called stego-object(s).
(ii) To transform the stego-object from spatial domain to frequency domain using DCT.
(iii) To compress the frequency domain stego-object using quantization and run length coding to generate a secure stego object.

Assumptions:
(i) Cover and payload objects are raw images of arbitrary size.
(ii) The LSBs of the cover image is utilized to embed the payload to minimize distortion in the cover image.
(iii) Stego-object is transmitted over the noiseless channel.

Let c be the cover image, h be the hidden image, bee stego image. Let P be the number of bytes in cover image which are used
to store one byte of the hidden image. Let ifile be the input file and c file be the output file.

Secure Data Splitting and Embedding Algorithms

4.1 Secure Data Splitting Algorithm:

The algorithm which is used to split the secure Data into two different shares is given below:
(INPUT: Secret Data
OUTPUT: Two different secret shares of input data)
Step1: Start
Step2: Clearing variables, closing figures and Clear output screen.
Step3: Read input secret data or color secret image in 256 × 256 standard. If image is not in this standard then convert it into 256 × 256 standard and also conversion RGB into Binary image.
Step4: initializing the two different shares with pixel values zeros and the width of each share is twice than the width of secret data.
Step5: finding all the white pixels indexes i.e. pixel values ones, in the secret data and for every white pixel value we store the required values in each of the share.
Step6: finding all the black pixels indexes i.e. pixel value zeros, in the secret data and for every black pixel value we store the required values in each of the share.
Step7: Overlap these two shares to check the visual cryptography.
Step8: Stop

4.2 Data Embedding Algorithm:

The steps involved in the Data Shares Embedding algorithm using Least Significant Bit based technique are given below.
(INPUT: Two different Shares (Share1 and Share2) from Algorithm 4.1 and two cover images (Image1 and image2)
OUTPUT: Two Stego Image)
Step1: Start
Step2: Read two shares and two cover images. Convert color image into gray
Step3: Check that the shares are not too large for images.

```
 if (maximum length of share> maximum length of  image)
 Error (' shares cannot be embedded in the given images bigger images are
required") and exit
            end if
```

Step4: Embedding share1 into the last three LSB's of the image1 intensity

```
        Set k=1
         for i=1:height of image1
        for j=1:weight of image1
```

```
          if k <= size of share1
 sum=0;
          sum=sum+4*share1_vector(k);
                    k=k+1;
        if k<= size of share1
       sum=sum+2*share1_vector(k);
                    k=k+1;
end
if k<= size of share1
      sum=sum+1*share1_vector(k);
k=k+1;
end
if image1(i,j)+sum < 255
embed_image1(i,j)=image1(i,j)+sum;
else
image1(i,j)=image1(i,j)-sum;
 end
else
   i=height of image1;
  j=weight of image1;
end
end
end
```

Step5: Repeat Step4 for embedding share2 into the last three LSB's of the image2 intensity.

Step6. Computing the difference between original image and Embedded image

Step7: Calculating the PSNR of these Embedded Images using equation 4.1.

Step8: Stop.

4.3 Computing Peak Single to Noise Ratio (PSNR):

The Peak Single to Noise Ratio (PSNR) is a common measure of the quality of Embedded Image.

Calculating PSNR using following formula:

$$PSNR = 10\log_{10}\left(\frac{(255)^2}{MSE}\right)db$$

(4.1)

The mean square error (MSE) of two images of N x N pixels is defined as:

$$MSE = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\left(p_{ij} - p'_{ij}\right)^2$$

(4.2)

Where Pij is the original cover image value and p'_{ij} is the embedded image pixel value. The higher the pixel value the better the quality of the reconstructed image.

Flow Graph of the Proposed Method

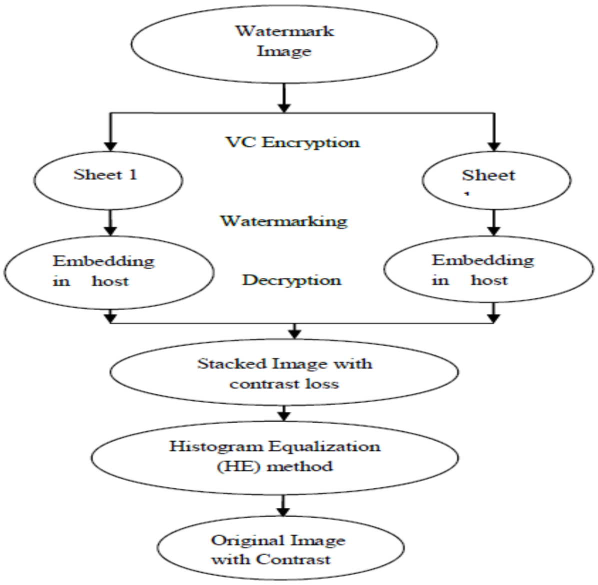

Figure 3. Flow graph of proposed scheme

5 CONCLUSION

In this paper, we have proposed a new method for detection of LSB matching steganography, and tested its performance on a database of uncompressed gray scale images. The main merits of our method are as follows.

(1) According to the properties of LSB matching, we find a novel discrimination rule to distinguish the cover and stego images, in which only the least two significant bit planes need to be considered.

(2) Since the alteration rate is a dimensionless discriminator, we can use our scheme to detect the given images with different size.

(3) It is easy to combine our technique with Harmsen'sor Ker's to design a more reliable detection rule.

6 REFERENCES

[1]. Alfred J, M et al., 1996.Hand book of applied Cryptography. First edn.Ali-al, H. Mohammad, A.2010.

[2]. Digital Audio Watermarking Based on the Discrete Wavelets Transform and Singular Value Decomposition, European Journal Of Scientific Research ,vol 39(1), pp 231 239.Amirthanjan,R.Akila,R&Deepikachowdavarapu, P., 2010.

[3]. A Comparative Analysis of Image Steganography, International Journal of Computer Application, 2(3), pp.2-10. Arnold, M. 2000.

[4]. Audio watermarking: Features, applications and algorithms, proceeding of the IEEE International Conference on Multimedia and Expo, pp 1013-1016.
Bandyopadhyay, S.K., 2010.

[5]. An Alternative Approach of Steganography Using Reference Image. International Journal of Advancements in Technology, 1(1), pp.05.11 Bloom, J. A. et al., 2008.

[6].Digital watermarking and Steganography .2nded.MorganKaufmann.Bishop, M., 2005.

[7]. Introduction to computer security.1sted.Pearson publications.2ndEd. Elsevier. Cummins, J. Diskin, P. Lau, S. & Parett, R., 2004.