© 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Enhanced Multi Level Secret Data Hiding

Swati S Patil, Prof. Sangeetha Goud
Department of Electronics and Communication, SDM College of Engineering and Technology, Dharwad, Karnataka, India

ABSTRACT

In this paper we present enhanced multi-level secret data hiding which integrates two different methods of encryption namely visual cryptography and steganography. First as a pre-processing step we are using a method called halftoning which is used to reduce the pixels and simplify the processing. After that visual cryptography is performed that produces the shares which forms first level of security and then steganography in which we hide the shares in different media like image, audio and video. Hence we get the enhanced multi-level secret data hiding which improves the security over the network.

Keywords: Steganography, visual cryptography, cover media, secret data, shares, stego key or password

I. INTRODUCTION

In today's world most of the applications requires online transactions over the computers. These make use of transferring data over the network. In core banking and internet banking systems we need to safeguard our account numbers, passwords or any confidential data from hackers that needs to be transferred over the network needs strong level of security. Hence to safeguard those transactions over the network we need a secure security model which will not allow hackers to hack the secret information easily. So in this perspective we are combining these two methods namely visual cryptography and steganography to get multi-layer information hiding.

As a preprocessing step we are using a method called halftoning [1] in which we are reducing the number of pixels so that further processing becomes easy. It is the representation method in which we are representing the continuous tone image in the form of binary 1's and 0's. In this we insert a dot where there is 1 in the image and leave the pixel position as it is if the pixel is 0. Hence the halftoned image is like the distribution of dots in the place of pixels. But when seen from far view this image looks like the normal image without dots. Hence by doing this many bits pixels reduce to a single bit pixel in the form of binary 1 or 0 and simplifies further processing.

Visual cryptography [2] is the encryption method in which we are dividing the image into the pieces where these pieces are called as shares. We are randomly distributing the pixels in the shares. The important advantage of this method is its simplest decoding. For encoding we are just dividing the image into shares using random number generator. And in decoding we just overlay those shares on one top of the other we get the original image v are stacking the shares on one top of the other to get the original image back. It uses the logical bit XOR function or just human visual system (HVS) to stack the shares back with perfect alignment and give the original image back.

In steganography [3] we are using the technique of hiding the hidden data. Here using this method the hacker remains unaware of the communication and safeguard the confidential data. In steganography we are hiding the data in another data. In this project we are hiding the shares in various cover medias of image, audio and video. It means using LSB technique we are inserting the secret data in the least significant bit position of the cover media.

II. METHODS AND MATERIAL

Related Theory

A. Literature Survey

Naor and Shamir [4] proposed a algorithm called as (k, n) threshold secret sharing scheme in the year 1994 which is now popularly called as visual cryptography (VC), in which the image is divided into n shares and k shares are sufficient to decrypt the original image. Here decryption is very simple and requires the human visual system (HVS) or the logical bit XOR functions. Hence unlike other cryptography techniques which require complex computations, this system requires only simple HVS. The shares generated by visual cryptography are the collection of random pixels and thus will be meaningless if used alone and do not reveal any information regarding the original image. All the shares are needed or a threshold number of shares are needed to properly decrypt the image. Till the year 1997 all the visual cryptography schemes proposed were only for black and white images. Verheul and Van Tilborg proposed the first colour visual cryptography scheme.

Hsien-Wen Tseng, Feng-Rong Wu, and Chi-Pin Hsieh proposed a different method of hiding data in binary images in the year 2007. Here the cover image that is binary is divided into equal sized blocks of n x n so that each blocks of the cover image are embedded a secret data bit except for blocks of completely black and white pixels. Beenish Mehboob and Rashid Aziz Faruqui proposed the art and science of steganography in the year 2008. They used a technique which uses least significant bit for embedding the data. In 2012 Ankit Chaudhary and JaJdeep Vasavada had planned to propose a scheme to hide text messages in the RGB images. Kousik Dasgupta & J.K. Mandaland, Paramartha Dutta thought of proposing the method of video steganography using LSB technique in the year 2012. Visual cryptography [5] requires two transparent images or shares which individually do not reveal any information. In that one transparency consists of truly random pixels and another consists of secret information. Both the transparencies are needed to decrypt the original image back.

B. Multi-Level Security Scehems

There are three techniques used in this project namely halftoning, visual cryptography and steganography

1) Halftoning Method

There are various methods available for halftoning like constant threshold halftoning, ordered dithering, block replacement and error diffusion. In out paper we are using error diffusion method in which we quantify each pixel based on the neighbourhood operation. The schematic diagram of the error diffusion method is shown below in the figure 1

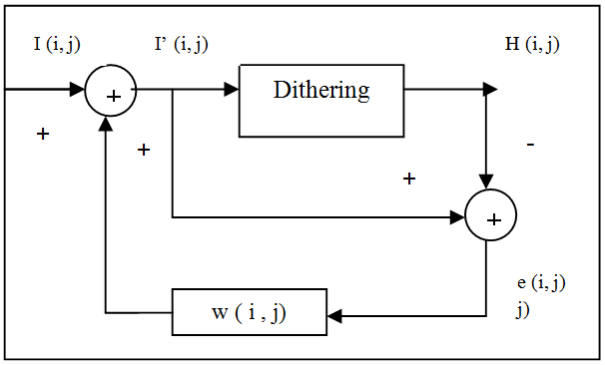

Figure 1: Error Diffusion Halftoning Method

This method moves in the raster form through the original image. It starts from the left most first pixel in the image matrix to the rightmost last pixel. The value of the pixels in the input image is set according to the constant threshold method where 1 and 0 are set in the output image according to the value of the threshold fixed. Because we are assigning the value 1 or 0 in H image based on I image, there is a difference between I and H image. Hence the difference called error 'e' of I and H is calculated. Then this error calculation is pushed forward to the yet to be processed pixels. In which order the error calculation moves in the image is decided based on weight matrix 'w'. This error diffusion weight matrix is multiplied along with error and added to the input image I.

Hence like this the above steps are calculated for the pixels in the input original image until all the pixels in the original image are processed in the raster order and finally the error diffused image is obtained.

2) Visual Cryptography Method

Visual cryptography is a cryptographic method [6] in which we divide the original image into shares such that decryption is as simple as just stacking the shares to get back the original image. Unlike other methods for encryption this scheme does not require complex computations or a computer for decrypting but only

requires the human visual system or XOR function to overlay the shares on one top of the other.

The popular method for visual cryptography is secret sharing scheme which was proposed by Moni Naor and Adi Shamir in the year 1994. According to their method the image was divided into n shares so that all the n shares are required for decryption and if only n-1 shares are available then that does not give the original image back. When all the n shares were overlaid in perfect alignment then the original image appeared. Using this idea we can divide the image into two transparencies where the first one consists of purely random pixels and second one consisting of secret information. In the simple (2, N) threshold secret sharing scheme [7] we are diving the image into N shares such that only 2 of the shares are required to be overlaid to get back the original image back. For example in a (2, 2) threshold secret sharing scheme image is divided into 2 shares and both the shares are required for decryption. This (2, N) threshold secret sharing scheme can cheated. By knowing the underlying distribution of pixels the hackers are adding extra shares which combine with the original shares and hence form the new hackers secret image. The visual cryptography is given by following setup; the secret image consists of black and white pixels where each pixel is treated independently. To encode we divide the image into n shares such that every pixel in the shares are now subdivided into n black and black subpixels. To decode we are taking the subset of the shares, if that subset is qualifying then by stacking those shares gives the original image back.

3) Steganography Method

Steganography is the art and science of invisible communication of messages over the network. The word steganography us derived from the Greek words [8] "stegos" means cover and "graphia" means writing which means "covered writing". Steganography has the long Greek history. The Greek nobleman Histaeus needed to communicate in Greece with his son-in-law [9]. And he used the technique of steganography by shaving the head of his most trusted slave and writing the secret message on that scalp. Then when the hairs grew back he was dispatched with the secret message. In this way it is extremely difficult to detect and provide a reliable communication.

The elements required for steganographic algorithm are [10]

- Cover media (C)
- Secret image (S)
- Stego function (Fe)
- Optional stego key or password

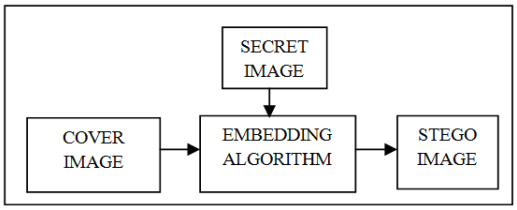

Figure 2 : Steganography Algorithm

The method we are using in this paper is the spatial domain method known as least significant bit insertion method or also called as LSB method. In this method we are first converting the secret data bits in the form of array. Then that array of data is inserted one by one in the least significant bit position of the cover media like image, audio or video. Hence the number of least significant bits chosen will decide the amount of degradability of the cover media. That is if more number of cover media bits are replaced by secret data then the stego media looks different from cover media and can be detected.

C. Working of Multi-Level Security Scheme

A) Encoding Method

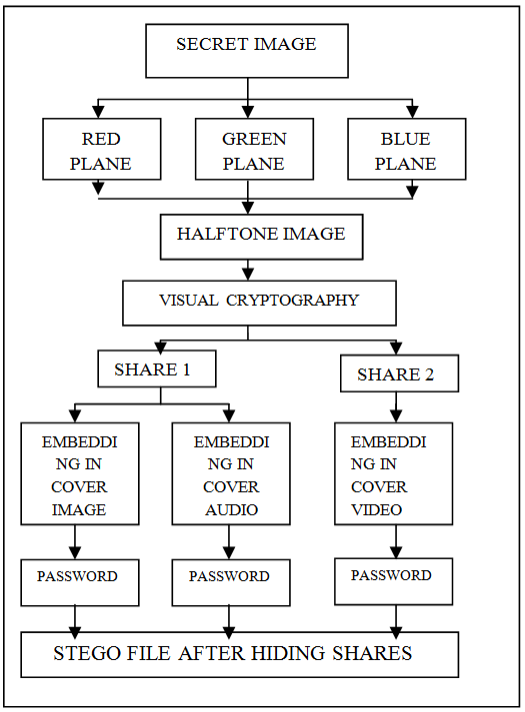

Figure 3: Encoding Process

The above block diagram in figure 3 shows the encoding process [11] where we are first halftoning the secret image, then performing visual cryptography and finally hiding the shares produced in the media like image, audio and video. Below are the steps given for each block in the figure 3:

1) First secret colour image such that the size should be less than cover file.
2) Colour image is basically a R plain, G plain and B plain.
3) Apply Floyd & Steinberg filter (half tone), to RGB plains. To convert image intensity to logical value.
4) Output of half tone image consists of logical value (0/1)
5) Halftone image is fed as input to visual cryptography, binary data is split into two shares and secret halftone information is split into two shares.
6) Cover image is selected, two plains of the first share are embedded in LSB (least significant bit) of cover image.
7) Password can be optionally entered, output image we call stego image.
8) Next audio file is selected and third plain share 1 is embedded in the audio file and password is entered.
9) Video is selected as cover media, all planes of second share are embedded into selected frame from video file.

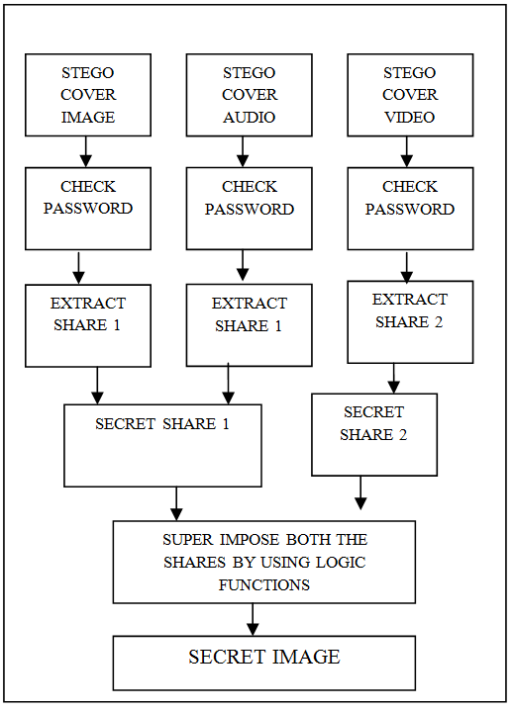

Figure 4: Decoding Process

The decoding process shown in the figure 4 above consists of the procedure in the reverse order of the encoding process.

The following are the decoding steps.

1) Enter password, & verify password in the stego media.
2) If password matches then extract secret share plains from cover image in the LSB position. If password does not match then stop the process.
3) After extracting secret bit stream array, convert array into matrix or image.
4) Enter password and verify password in stego audio.
5) If password matches extract secret share plains from cover audio in the LSB position and if the password does not match stop the process.
6) After extracting secret bit stream array, convert array to matrix.
7) Output obtained is secret share1.
8) Enter password and verify password in stego video.
9) If password matches extract secret share plains from cover video, from selected frame in LSB position, if password does not matches stop the process.
10) After extracting secret bit stream array, convert array to matrix to get output share 2.
11) Super impose share1 and share2 to get secret image.

III. RESULTS AND DISCUSSION

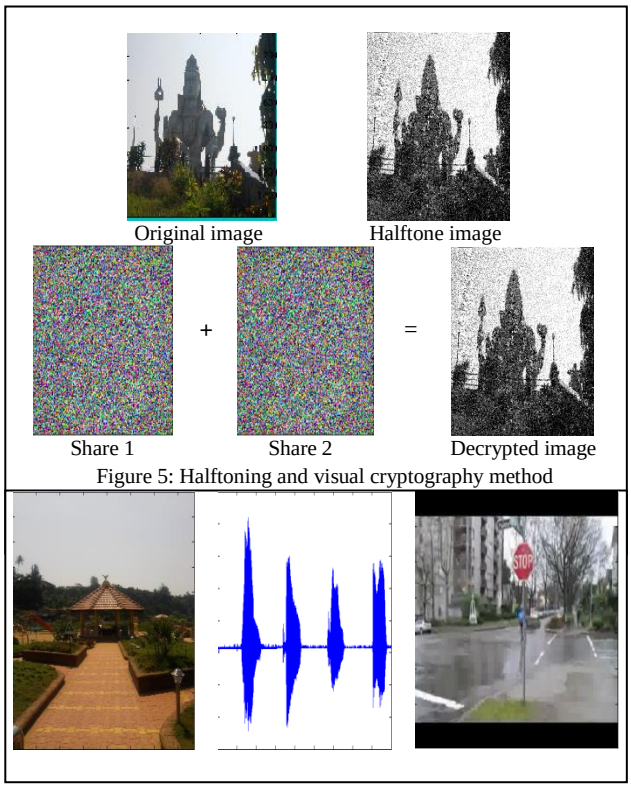

Figure 5: Halftoning and visual cryptography method

Figure 6: Stego image, stego audio and stego video

IV. CONCLUSION

Hence we can conclude that using visual cryptography and steganography we get the advantage of multi-level security. Using only visual cryptography gives the simplest decoding ever possible but at the same time will provide unreliable security because of the simple decoding technique. So in this perspective we also combine steganography algorithm using LSB insertion method which enhances the single level security. This steganography is the method of hiding the hidden data that is making the communication itself invisible by hiding data in another media. By using this reliable communication can happen because hacker is unaware of the communication. Hence multi-level enhanced security is achieved.

V. REFERENCES

[1] Jithesh K , Dr. A V Senthil Kumar," Multi Layer Information Hiding -A Blend of Steganography and Visual Cryptography", Journal of Theoretical and Applied Information Technology, 2005 – 2010

[2] M. Wherate, Dr. S. Sherekar, Dr. V. M. Thakre, " Two Layer Security Using Visual Cryptographyand Steganography" , International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, April 2015

[3] Khalil Challita and Hikmat Farhat," Combining Steganography and Cryptography: New Directions", International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 199-208, ISSN 2220-9085, The Society of Digital Information and Wireless Communications, 2011

[4] Deepti B. Khasbage, Prof. DR .P.R. Deshmukh, "Data Hiding & Visual Cryptography:A Review", International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 6981-6984

[5] Rahul Kumar, Ajit Pratap Singh, Arun Kumar Shukla, Rishabh Shukla , "Enhancing Security using Image Processing", International Journal of Innovative Research in Science,Engineering and Technology, Vol. 4, Issue 4, April 2015

[6] Yasir Ahmed Hamza," Securing Image Steganogarphy Based on Visual Cryptography And Integer Wavelet Transform", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 12, Issue 6 (Jul. - Aug. 2013), PP 60-65

[7] S.Premkumar, A.E.Narayanan , "Steganography Scheme Using More Surrounding Pixels combined with Visual Cryptography for Secure Application", International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012

[8] Prof. Samir Kumar Bandyopadhyay1 and Barnali Gupta Banik2," Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique", International Journal of Emerging Trends & Technology in Computer Science, Volume 1, Issue 2, July – August 2012

[9] Jagvinder Kaur, Sanjeev Kumar," Study and Analysis of Various Image Steganography Techniques", IJCST Vol. 2, Issue 3, September 2011

[10] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, "Steganography Using Least Significant Bit Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp. 338-341

[11] Ravindra Gupta, Akanksha Jain, Gajendra Singh," Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics", International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4366 – 4370