A STENO HIDING USING CAMOUFLAGE BASED VISUAL CRYPTOGRAPHY SCHEME

[1]P. Arunagiri, [2]B.Rajeswary, [3]S.Arunmozhi and [4]K.Priethamje vithya

[1,2,3,4]*Sri M1anakula Vinayagar Engineering College, Pondicherry University*
[1]*arun_qmm@rediffmail.com,*[2]*rajeswary26@gmail.com,*
[3]*s_arunmozhi@rediffmail.com,*[4]*lvk_prietham@yahoo.co .in*

ABSTRACT

This work deals with an Integrated Secured Data Communication Using Visual Cryptography. Idea of visual cryptography is to hide a secret image in different images called shares or cover images. This concept achieves lossless recovery and reduces the noise in the cover images and also enhances the quality of cover images without increasing the computational complexity. There are three levels of security which is highly safe and difficult to trace out by unauthorized person. Initially the text message or plain text which is converted into cipher text using RSA algorithm. In the first level security, the cipher text is hidden in the secret image. Next in the second level security, the secret image is encrypted. In this process the LSB technique is used. In the third level security, the video file is converted into several frames and the secret image is hidden in the video file frames.

Keywords – Cryptography, Image, Frames, message, Camouflage

1. INTRODUCTION

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.

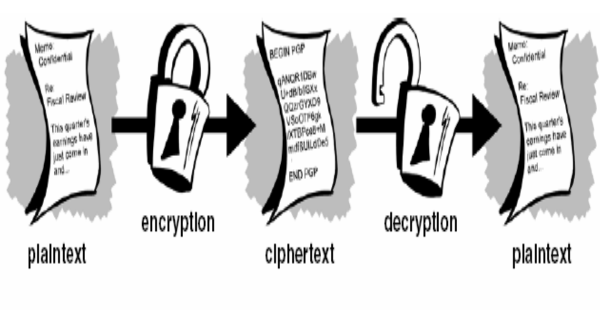

Figure.1 General Block Diagram of Cryptography

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key, a word, number, or phrase to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

2. 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 Moni Naor and Adi Shamir in 1994 [1]. 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. Fig 1 shows the working of visual cryptography. We can achieve this by using one of following access structure schemes [8].

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.

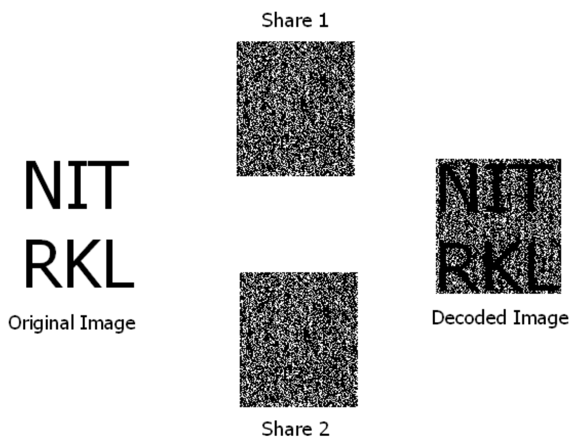

Figure.2 working of visual cryptography

2.2. Basic approach

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.

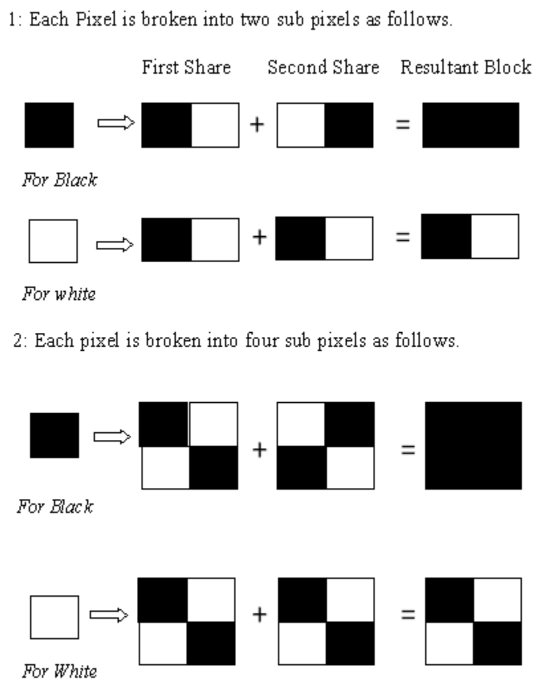

Figure.3 Visual Cryptography

3. PROPOSED ALGORITHM

In this section the proposed improved visual cryptography scheme for secrete data hiding (VCSDH) which is a modified version of Existing Data hiding in halftone images using conjugate ordered dithering (DHCOD) algorithm. Here using three levels of security which is highly safe and difficult to trace out by unauthorized person. The proposed scheme achieves lossless recovery and reduces the noise in the cover images without adding any computational complexity.

3.1 VCSDH algorithm

A secrete data is hidden into cover image and considered it as ten numbers. The data hidden image is steno image. This ten number of steno image is hidden into a video file which consist of ten frames and this hidden file is shared by ten person to provide security and make difficult to trace out by unauthorized person.

Step1: considered a secrete data and Encipher the data using receiver public key as per RSA algorithm.

Step 2: Select an image as cover image to embed the encipher data into the image.

Step 3: Transmit this Data hidden image that is stenography image along with video file.

Step4: Recover the steno image from the video file and recover cipher from the steno image.

Step5: Decipher the text using its (receiver) own private key and recovered cover image and secret data.

3.2 Hiding Algorithm

For a 2 shares out of 2 schemes, the construction can be described by a collection of 2x9 Boolean matrices *C*. If a pixel with color *k= (k1k2…k8)2* needs to be shared, a dealer randomly picks an integer r between 1 and 9 inclusively as well as one matrix in C.

3.3 Steps for Hiding Algorithm

- Take a colored secret image I_{HL} of size *HxL* and choose any two arbitrary cover images O^1_{HL} and O^2_{HL} of size *HxL*.
- Scan through I_{HL} and convert each pixel I_{ij} to an 8- bits binary string denoted as *k= (k1k2…k8) 2*.
- Select a random integer r_p, where 1≤rp≥9 for each pixel Iij.
- According to r_p and *k* for each pixel, construct S.
- Scan through O1 and for each pixel of color k1p, arrange the row "i" in S as a 3x3 block B1p and fill the sub pixels valued "1" with the color k1p

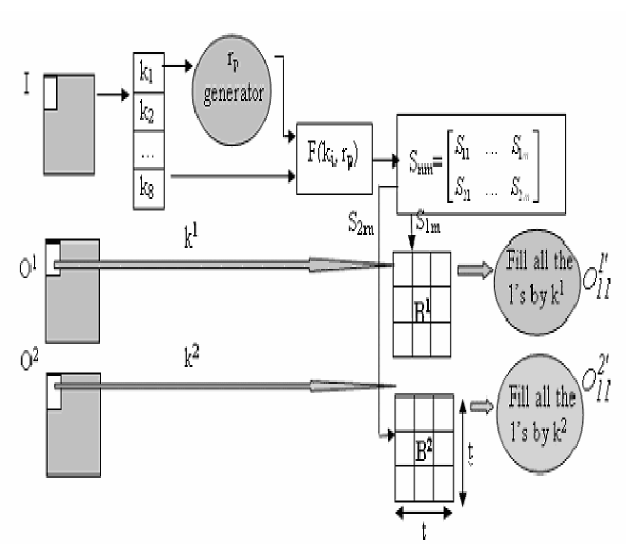

Figure.4 Hiding Algorithm Flowchart

- Do the same for O^2 and construct $B^2{}_p$. The resulting blocks $B^1{}_p$ and $B^2{}_p$ are the sub pixels of the p^{th} pixel after the expansion
- After processing all the pixels in IHL, two camouflage colored images $O^{1'}$ and $O^{2'}$ are generated. In order to losslessly recover IHL, both O1' and O2' as well as a sequence of random bits R= {r1, r2, …, r |I|}are needed.

Figure 4.1 describes the (2,2) scheme for hiding one pixel. This process is repeated for all pixels in IHL to construct both camouflage images $O^{1'}$ and $O^{2'}$.

3.4 Recovering Algorithm

In order to recover the secret image in a 2 out of 2 scheme, both camouflage images $O^{1'}$, $O^{2'}$ as well as the string of random bits R are required for the recovery process (Fig. 6.2). The camouflage images are *t* time bigger than IHL due to the expansion factor of sub pixels.

3.5 Steps for Recovery 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 rp corresponding to the first encrypted pixel
- Input S_r and r_p to the *F(.,.)* function corresponding to equation (1).
- Recover k_p, the first pixel in I_{HL}
- Repeat for all 3x3 blocks in $O^{1'}$ and $O^{2'}$

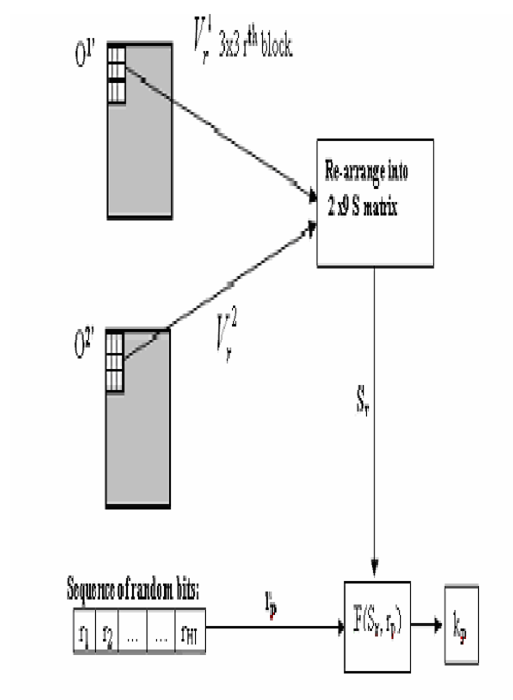

Figure.5 Recovering Algorithm Flowchart

4. Merits of Proposed Scheme

Proposed scheme provides a high-level security. Here using three levels of security which is highly safe and difficult to trace out by unauthorized person. The proposed scheme achieves lossless recovery and reduces the noise in the cover images without adding any computational complexity.

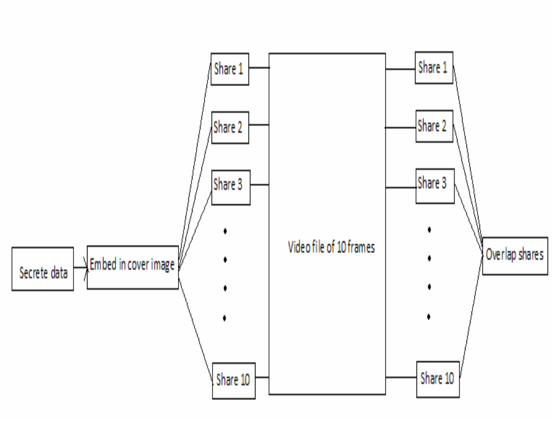

Figure.6 Structure of proposed scheme

5. Simulation Results

Figure.7 shows the steno image that is ciphered text is embedded into cover image shown in right side figure.

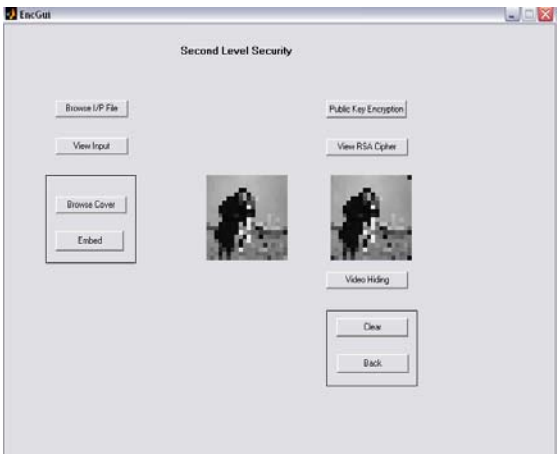

Figure.7 Steno Image

Figure.8 shows ten number of shares which are shared by ten members to provide high security from the unauthorized person.

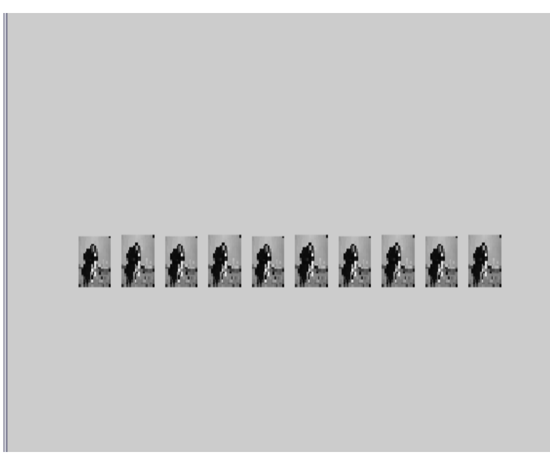

Figure.8 ten number of shares

Figure.9 shows stacked file which is stacked the ten numbers of shares.

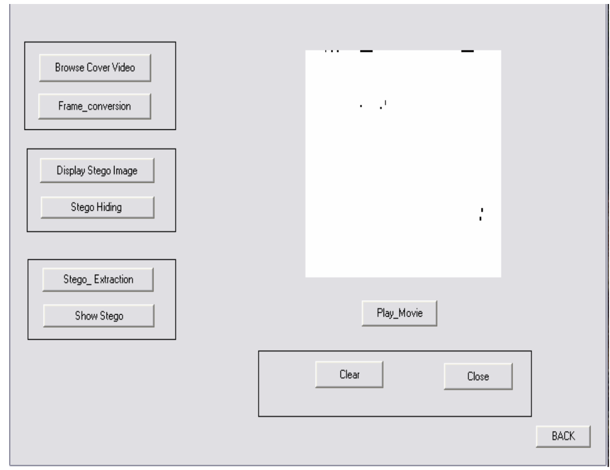

Figure.9 stacked file

6. CONCLUSION

A data embedding technique for data hiding within a MPEG transparent video system was designed and tested successfully. Here merge both video compression and data hiding techniques such that it can be applicable for both consumer and defense applications.

7. REFERENCES

1. A Novel Visual Cryptography Scheme, Debasish Jena1, Sanjay Kumar Jena2, Centre for IT Education, Biju Pattanaik University of Technology, Orissa 751010, India, Department of Computer Science & Engineering, National Institute of Technology Rourkela, Orissa 769 008, India,2010.
2. D. Stoleru (2005), Extended Visual Cryptography Schemes, Dr. Dobb's, 377, October 2005
3. M. Pazarci, V. Dipçin, "A MPEG2-Transparent Scrambling Technique", IEEE Transactions on Consumer Electronics, Vol.8, No. 2, May 2002. Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC'03) 1530-1346/03 $17.00 © 2003 IEEE
4. D. Stinson (2002), Visual Cryptography or Seeing is Believing, pp presentation in pdf.
5. B.D. Pettijohn, M.W. Hoffman, and K. Sayood, "Joint source/channel coding using arithmetic codes," IEEE Trans. Commun., vol. 49, no. 9, pp. 1540–1548, Sept. 2001.
6. C. Chang, C. Tsai, and T. Chen, A new scheme for sharing secret color images in computer network. In the Proceedings of International Conference on Parallel and Distributed Systems, pages 21–27, July 2000.
7. S. Lee, "Foveated video compression and visual communications over wireless and wireline networks",

Ph.D. Dissertation, The Univ. of Texas at Austin, May 2000.

8. C. M. Privitera and L. W. Stark, “Algorithms for Defining Visual Regions-of-Interests: Comparisons with Eye Fixations”, IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 22, no. 9, Sep. 2000.

9. P. Bahl, I. Chlamtac and A. Faragó, “Optimal Resource Utilization in Wireless Multimedia Networks,” Proceedings of the IEEE Conference on Communications, Montreal, Canada (June 1997).

10. C. Boyd, J. Cleary, S. Irvine, I. Rinsma-Melchert, and I. Witten, “Integrating error detection into arithmetic coding,” IEEE Trans. Commun., vol. 45, no. 1, pp. 1–3,Jan. 1997.