A Visual Crypt Stego Approach with Randomized Puzzle Block Generation for Highest Secret Sharing

Dr. D.Devakumari
Assistant Professor, Department of Computer Science, Government Arts College, Coimbatore, Tamil Nadu, India.

K.Geetha
M.Phil Scholar, Department of Computer Science, Government Arts College, Coimbatore, Tamil Nadu, India.

Abstract – Data security is the major concentration of the current network scenario. The data security can be performed using Cryptography and Steganography techniques. To improve the security, the proposed system develops a visual cryptography with the Steganography approaches. This performs the data hiding process in the sliding puzzle blocks. Hiding some secret information inside a video. The addition of this information to the video is not recognizable by the human eye as the change of a pixel color is negligible. This project aims to provide an efficient and a secure method for video Steganography. The proposed system provides a novel effective scheme that is named as RBS (Randomized Block Stego), which is a new visual cryptography technique for data hiding with improved security features. The proposal has three main contributions such as, Randomized block stego scheme embedded with the puzzle blocks, Sequential sliding puzzle substitution techniques and Random color puzzle block verification. The proposed method creates an index for the secret information and the index is placed in a randomized puzzle block generated from the video. With the help of randomized puzzle block index, the frames containing the secret information can locate. Hence, during the extraction process, instead of analyzing the entire data, the frames containing the secret data are analyzed with the help of index at the receiving end. When steganographed by this method, the probability of finding the hidden information by an attacker is lesser when and it is effective in terms of computation overhead when compared to the normal method of sequential methods. It also reduces the process and time taken for the extraction process by deploying the sliding puzzle blocks.This RBS scheme have developed as a client server architecture using C#.Net, the experimental results shows, the proposed system extracts and preserves the carrier media with high security. But in the existing visual cryptography techniques, it failed to extract or concentrate the carrier media security.

Index Terms – Cryptography, Steganography, Visual Cryptography, puzzle block, data security.

1. INTRODUCTION

Digital information and data are transmitted more often over the Internet now than ever before. The availability and efficiency of global computer networks for the communication of digital information and data have accelerated the popularity of digital media. Digital images, video and audio have been revolutionized in the way they can be captured, stored, transmitted and manipulated, and this gives rise to a wide range of applications in education, entertainment, media and military, as well as other fields. Computers and networking facilities have become less expensive and more widespread. Creative approaches to storing, accessing and distributing data have generated many benefits for the digital multimedia field, mainly due to properties such as distortion-free transmission, compact storage and easy editing [1]. With the increasing dependence on computers at all levels, personal and sensitive information is increasingly being stored and transmitted using computer systems and networks every day. This revolution, however, has brought with it new threats and computer crimes as evidenced by the increased number of computer attacks and break-ins. Replicating important information will give greater chance to intruders to access it. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality (secrecy), authenticity, integrity and non repudiation [2]. Encryption was the first cryptographic operation used to ensure secrecy or confidentiality of information transmitted across an insecure communication channel. The encryption process gets a piece of data, which is known as plaintext and translates it into a cryptogram called as cipher text using a cryptographic key. Decryption is the reverse operation of encryption. The receiver who holds the correct secret key can recover the message (plaintext) from the cryptogram (cipher text)[3].

2. PROBLEM DEFINITION

Data security is the major research area of the current networks. Due to the huge improvements of the network and Medias, the digital data size increases tremendously. The cryptography and steganography techniques are widely used for data security [4]. However, the data security schemes need more process and steps to perform high security. Visual cryptography is such approach which needs less procedure to deploy higher security. However, the visual cryptography techniques are gaining less attention due to its security level [5][6]. The usual security systems have the following challenges.

1) Every data security framework needs high and strong keys to provide secure process like encryption, decryption, encoding

and decoding. These keys are may need high memory and processing time.

2) While considering the image steganogrpahy under the visual cryptography, it doesn't consider the carrier media at the time of extraction.

3) If the carrier media need to be extracted with out loss, then there is no proper mechanism under visual cryptography techniques.

To overcome the above challenges, the proposed system effectively combines the visual cryptography and seganography for successful data transmission.

3. PROPOSED SYSTEM

Data security with less resource requirements and less human interaction is always an interesting proposal. In the proposed system a fresh unique scheme of data hiding on color image sliding puzzle based visual cryptography is presented. The proposed system is a hybrid and randomized technique, which poses color image with random puzzle bloc to hide the data. This integrates the visual embedding scheme for secure data management and secret sharing. The process and functions involved in the proposed system is discussed. The proposed visual hiding technique contains three parts which are as follows.

- Data encryption
- Randomized data embedding and puzzle block generation
- Data extraction.

The data owner encrypts the original text content and embeds the data into the puzzle blocks randomly using standard randomized ciphers with hash keys to produce an encrypted puzzle blocks. Then, the data-hider can embed the additional data into the encrypted puzzle block by using random puzzle block verification method, without any further overhead. At the receiver end, the hidden data extraction can be accomplished either in encrypted or in decrypted version.

The fig 1.0 represents the overall process of the proposed visual cryptography scheme. The sender initiates the data hiding process by selecting the secret text and the video. To perform high security, the puzzle blocks are created from a huge set of frames, which extracted from the video. The frame extraction process gives the set of images at every second. If the video is a two second video, then 120 frames will be extracted. From the 120 frames, the random blocks in every single image are captured and the random block will hold a bunch of secret text message. This kind of data security gives the high security with less human interaction for retrieving it. To perform the extraction process, the substituted codes are verified automatically.

In each case, it is important to note that the bits should maintain this capacity in every coded bit stream, and that it cannot be envisaged to consider cases where given configuration of bit stream will allow immediate or delayed resynchronization. The synchronization of the data should be properly performed, then only the extraction process will be appropriate.

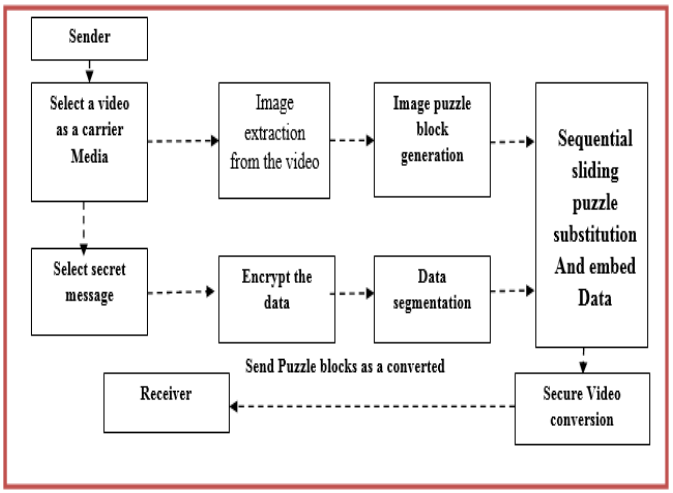

Fig 1.0 the overall process involved with the Proposed System

4. METHODOLOGIES IN THE PROPOSED SYSTEM

The proposed system provides a novel effective scheme which is named as RBS (Randomized Block Stego) for data hiding with improved security features. The followings are the main contribution of the proposed system.

1. Randomized block stego scheme embedded with the puzzle blocks
2. MD5 hashing technique
3. Sequential sliding puzzle substitution
4. Random color puzzles block verification.

The proposed system aims to develop a high security secret sharing using visual cryptography and image steganography techniques.

4.1 RBS: [Randomized Block Stego]:

The first contribution of the proposed system is the creation of new data hiding scheme. Unlike traditional visual cryptography and steganography algorithms the proposed system has multi level security which is not considered in the literature. The followings are the different phases of the proposed RBS scheme.

- Sliding puzzle block generation and RBS Embed process
- RBS extraction process

The system performs various security related algorithms along with the two phases.

A.RBS Phase 1:

The first phase of the proposed system is generating puzzle blocks with random process, which gets a video or image as input. To give higher security, the video will be taken as an input, and that will be segmented into different frames. The below algorithm represents the embedding process, which takes the video as an input. Initially the system performs frame extraction. Frame extraction is the process of splitting the whole video into different frames.

After the frame extraction, the system gets the user key for embedding and encryption process. The system performs the data encryption process based on the given key. And selects the data which the user need to hide (ie) the secret data. In this module using the MD5 algorithm convert the normal data to cipher text, earlier conversion methods convert the data's in bytes code format or in text format, that's not enough for healthy communication, MD5 algorithm make the secured data mechanism, converted data's are in cipher text format, so hacker cant able to read the exact data, this process only make the exact steganography Authentication process

Steps: (Embedding process)

Algorithm: Data Embedding Process

Step 1: Get the video file V.

Step 2: Split the video into frames

Step3: Read the input file (D) (which should be hide)

Step 4: Read the key bit (b) and perform encryption Encrypt (D(b))

Step5: For each frame [F] in the video V . Perform the following.

i. Split F into equal 9 blocks.
ii. Select randomized encrypted data E(D(b))
iii. Hide the data in randomized puzzle blocks.

Step 6: Perform the encryption process for video V.

Step 7: Do sequential Codeword Substitution process for Encrypted Video E(V).

Step 8: Transmit the encrypted stego video E(V) to the server.

Algorithm1: Data Embedding Process

B.RBS Phase 2:

The above embedding and extraction processes shows that, the data owner extracts a video and convert into frame and the real H.264/AVC puzzle block using typical stream ciphers with encryption keys to provide an encrypted puzzle block. Then, the data-hider can embed the extra data into the encrypted puzzle block by using codeword replacement method, without knowing the original video data. At the beneficiary end, the hidden data extraction can be accomplished either in encrypted or in decrypted version.

Steps: (Extraction process)

Algorithm: Data Extract process

Step 1: Get the encrypted video file EV.

Step 2: Perform extraction process using the sequential codeword verification

Step3: Read the input file (VD) (which has been hidden)

Step 4: Read the key bit (b) and perform decryption decrypt (D(b))

Step5: For each frame [F] in the video V . Perform the following.

i. Extract data block B and combine
ii. Verify the sequential sliding puzzle and display original video

Step 6: Perform the extraction process from every stego block.

Step 7: Do sequential codeword verification process to decrypted Video D(V).

Step 8: Extract and decrypt the hidden data and store.

Algorithm2: Data Extract process

5. IMPLEMENTATION AND RESULTS

The proposed visual cryptographic method based on the sliding puzzle block approach is implemented using C#.Net, which is a most GUI interface and effective programming tool for research and real-time applications. The proposed system has successfully implemented as a client server approach. The client can use the software to generate a sliding puzzle based secret sharing file, which can be passed by any media like email, Whatsapp and other social media. The data secrecy contains the several steps with less interaction with the users for the extraction. This facility provides an effective result in

both performance and application wise. The results obtained from the implementations are discussed.

5.1 Implementation steps:

1. Puzzle image segmentation from video:

2. Data Encryption

3. Data Hiding and Puzzle regeneration process

4. Video conversion

5. Extraction of original data and decryption process

5.2 EXPERIMENTAL RESULTS

To evaluate the performance of the proposed schemes, security, scalability execution time and storage are the main measurement of performance evaluation. Another criterion is cost evaluation. Cost evaluation involves storage and computation aspects. The performance of this proposed work RBS using improved block based sliding puzzle with game theory Scheme was compared with the existing approach LBS. The figure 2.0 below shows the results and embedding time comparison of the proposed system.

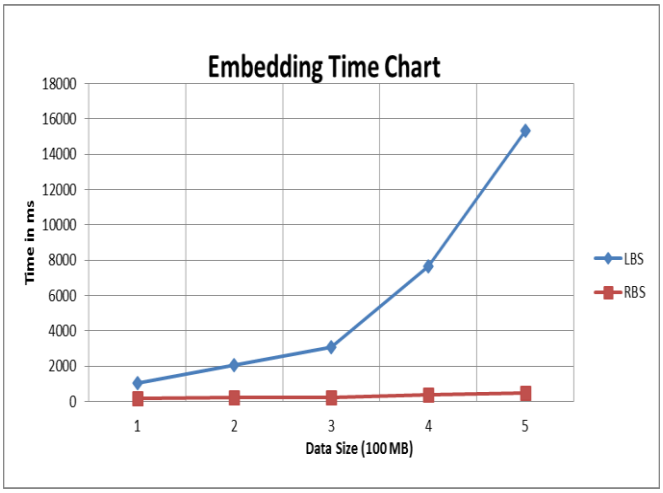

Figure 2.0 Performance of Embedding Time chart

6. CONCLUSION

Data security is more important in sensitive command passing environment such as organization secrets, military, government rules and policies should be transmitted securely. The proposed system implements a novel visual cryptography scheme for color images for effective and low overhead data hiding. The RBS which is defined as Random Block Visual Cryptography (RBVC), which is new storing idea with the use of improved block based sliding puzzle. Data encrypting and hiding in to the source media using color image sliding puzzle scheme is a new topic that has started to draw attention because of the low communication overhead and resource requirements in the network domain.

In this thesis, an algorithm developed to embed secret data in randomly selected image puzzle blocks. Initially the system splits the frame into n number of frames; each block of encrypted secret message will be hidden in the randomly selected block and the sequence of the keys is collected from the block index. Finally the system performs the video encryption process which is H.264/AVC bitstream is presented, which consists of video encryption, data embedding and data extraction phases.

REFERENCES

[1] Shilling, Cameron G. "Privacy and data security: new challenges of the digital age." *New Hampshire Bar Journal* 52.2 (2011).

[2] Naor, Moni, and Adi Shamir. "Visual cryptography." *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 1994.

[3] Yeager, C. Douglas. "Systems and methods for authorizing a transaction with an unexpected cryptogram." U.S. Patent Application No. 13/599,647.

[4] Dawen Xu, Rangding Wang, and Yun Q. Shi , "Data Hiding in Encrypted H.264/AVC Puzzle blocks by Codeword Substitution" in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO.

[5] Manika Sharma, Rekha Saraswat, "Secure Visual Cryptography Technique for Color Images Using RSA Algorithm", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 10, April 2013.

[6] Z. Zhou, G. R Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," in Proc. of IEEE International Conference on Image Processing, Barcelona, Spain,Sept 2003, vol. 1, pp. 521–52

[7] D. Madhav, "A Survey on Perceived Visual Quality and Secured Visual Cryptography Schemes".

[8] Praveen Kumar, "A Survey on Visual Cryptographic Schemes and their Comparative Analysis".