IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 66-73
www.iosrjournals.org

An efficient Secure Video Transmission using Secret-Fragment-Visible Mosaic Images

[1]Lakshmi Priya K.M ,[2]Smitha Suresh ,[3]Deepak P ,[4]Swapna Sasikumar
[1]*Final Year MTech, CSE SNGCE , Kadayiruppu, Ernakulam, Kerala, India*
[2]*Assoc.Prof. CSE SNGCE, Kadayiruppu Ernakulam, Kerala, India*
[3]*Assoc. Prof, ECE SNGCE,Kadayiruppu Ernakulam,Kerala, India*
[4]*Programmer,CSE SNGCE,Kadayiruppu Ernakulam,Kerala,India*

Abstract: *Nowadays videos from different sources are required to transmit through the web for very pertinent applications .These videos may contain confidential data so they must be protected during transmission to avoid leakage. To ensure the confidentiality of such videos an SVTSM system is proposed. The main essence of this methodology is taken from an existing image transmission technique called secret-fragment-visible mosaic image, which is created using small fragments of a given image to get a target image called as mosaic image. In the proposed system that actual video is embedded in to the mosaic video. The risk of transmitting a secret video data inside another video is very high. In the existing system, secret-fragment-visible mosaic image method applies only for the image data. But the proposed system adopted the same method for the video image. The process starts with dividing the video data into frames and then for each frame the algorithm applies. First the secret frame and corresponding target frame is divided into different fragments of equal size and transforming the colour characteristics of fragments of secret frame to the corresponding blocks of the target frame. The audio data of each secret image frames are shuffled using the scramble method for security purpose. To reduce the data to be embedded, Huffman encoding is also used in the proposed system using a secret key. The original secret video is extracted at the receiving end by applying the reverse process using the same secret key.*

Keywords: *Secret-fragment-visible-mosaic-image, Scrambling, Huffman encoding*

I. Introduction

Due to the advanced technologies the security/ secrecy of private or confidential data is a big problem in the present society. The confidential data includes documents, audio, image, video. Here mainly concentrating on secret video data. Many techniques are available for securely transmitting audio and image data. But securely transmitting a secret video data is not much common. In the existing work, an efficient technique for secure image transmission is used, which transforms a secret image into a meaningful mosaic image with the same size and looking like a preselected target image. The transformation process is controlled by a secret key, and only with the key can a person recover the secret image nearly losslessly from the mosaic image. The method is inspired by I-Jen Lai et al.[1], in which a new type of computer art image, called secret-fragment-visible mosaic image, was used. The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image preselected from a database. Using their method, the user is not allowed to select freely his/her favorite image for use as the target image. But these disadvantages are overcome, while keeping its merit in the newly introduces method. Here transforms a secret image into a secret fragment-visible mosaic image of the same size that has the visual appearance of any freely selected target image without the need of a database.

The proposed SVTSM method uses the Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations technique. The proposed method deals with the video data instead of image data in the existing system. The secret videos used for the surveillance systems and military etc are highly confidential, so the protection of such data has high importance in the real world. The secret video data is to be transmitted through a secure way in the method. So, the conversion of the video data into different frames is a task to be done as the pre-processing step. So here proposes a non patch based color transform in which embedding of data can be reduced and hence less distortion can be guaranteed. By creating mean and variance image and compress it instead of storing the values directly inside the target image the amount of data embedded can be reduced. The audio data is also handled using a scrambling method. Also applies a Huffman encoding technique or storing the data or retrieval process. This will result in reduction of distortion of the mosaic image. This method of secure video transmission can be used in many real time applications also.

II. Existing Methods

The image/ video data are transmitted securely using different techniques. Some of the methods are: Howard Cheng et al.[2] proposes, the processing time for encryption and decryption is a major bottleneck in real-time image and video communication and processing. Moreover, the processing time required for compression and decompression has to be considered, for processing the associated audio data, and for other processing such as video capture and display, contrast adjustment, and soon. The computational overhead incurred by encryption and decryption algorithms makes it impossible to handle the tremendous amount of data processed. Here proposes a novel approach called partial encryption to reduce encryption and decryption time in image and video communication and processing. In this approach, only part of the compressed data is encrypted. Partial encryption allows the encryption and decryption time to be significantly reduced without affecting the compression performance of the underlying compression algorithm. Although a large portion of the compressed data is left unencrypted, it is difficult to recover the original data without decrypting the encrypted part.

Zhenfei Zhao et al. [3] developed the secret sharing is a kind of popular used information encryption method. Although many secret sharing schemes are developed for reducing size of share, shares transmission is still a significant problem, especially in the transmission channels with limited bandwidth. In this work, the principle of progressive image transmission is adopted to transmit shares. That is, here incorporate secret image sharing with progressive transmission aiming to mitigate the burden on limited bandwidth channels with the high security of the secret image still maintained.

J.K. Mandal et al.[4] presented the steganography is a method to protect data from illicit attacks. The Steganographic algorithm hides a secret message in a cover medium like digital image, video, audio or even HTML code to avoid malicious eyes. To protect digital image document from unauthorized access information security and image authentication has become very important. The paper proposes a new secret message/image transmission scheme which emphasizing on the concept of multiple encryption where the secret message/image has been fabricated into the cover image through a hash function and without transmitting the stego data through (2, 2) visual cryptographic protocol, the shares are converted into meaningful images using embedded steganography and then transmitted. The cover, binary image act as signature to authenticate the secret message/image and instead of normal post encryption transmission, the embedded image is again encrypted through (2, 2) VCS to act as one time pad to provide higher security level and resulting shares are covered by separate meaningful images. Wei-Jen Wang et al. [5] analyses the major problem of publicity and openness is that malicious people can attack or steal personal data easily, even though the victims may put many efforts on privacy protection. Data hiding is one possible way to achieve better data and communication protection by hiding information into a media carrier to form a media file or an unrecognizable code stream.Vector quantization (VQ)-based data-hiding methods area subgroup of image data hiding. This paper focuses on the issues of data hiding for VQ-based images. It provides a state-of-the-art review for VQ-based data-hiding methods, the details of some representative methods, and comparisons of the different existing data-hiding methods for VQ-based images. Shan-Chun Liu et al.[6] conducted investigations on computer art image were the mosaic image is also a type. Each mosaic image is composed of many small identical tiles, such as squares, circles, triangles, and so on. Different from conventional mosaic images which have tiles all arranged in a fixed orientation, Hausner created a type of tile mosaic image by placing tiles to follow the edges in the input image to make the created art image look smoother. Another important criterion for art image creation is to limit the number of strokes so that the resulting image looks like an abstract painting, which comes from Haeberli. Some paintings of the Cubism style are dominated by line sand regions, to show abstractly a characteristic of the Cubism art—multiple-viewpoint.

Kai-Hui Lee et al. [7] proposes a method, visual cryptography (VC) is a technique that encrypts a secret image into n shares, with each participant holding one or more shares. Anyone who holds fewer than n shares cannot reveal any information about the secret image. Secret images can be of various types: images, handwritten documents, photographs, and others. Sharing and delivering secret images is also known as a visual secret sharing (VSS) scheme. The original motivation of VC is to securely share secret images in non-computer-aided environments; however, devices with computational powers are ubiquitous. Thus, sharing visual secret images in computer-aided environments has become an important issue today. Conventional shares, which consist of many random and meaningless pixels, satisfy the security requirement for protecting secret contents, but they suffer from two drawbacks: first, there is a high transmission risk because holding noise-like shares will cause attackers' suspicion and the shares may be intercepted. Thus, the risk to both the participants and the shares increases, in turn increasing the probability of transmission failure. Second, the meaningless shares are not user friendly. As the number of shares increases, it becomes more difficult to manage the shares, which never provide any information for identifying the shares.

Hirdesh Kumar et al. [8] presents, a new color image security scheme which comprises of deformation and reformation algorithm for color image. This scheme is based on key safeguarding as well as secret image sharing scheme. Here an idea from matrix calculation is taken for generating the key image using the secret color image and p securing images or shares (which are like secret) and reforming the secret color image using the key image and q securing images or shares is called (p, q) threshold scheme. There are two algorithms used mainly in this method, first one is for deformation at the sender side and other is for reformation of secret image at receiver side. The secret image is recovered without distortion and has correlation 1 as compared with the original secret image. By this scheme the secret image is retrieved from anywhere if the specified conditions are satisfied. There is lot of scope for future work like use this scheme for multiple secret images and reduce the space complexity. Develop a more complex and secure technique in which shares are ordinary images.

Mohammed A. Saleh et al. [9] develops the multimedia applications like sending and receiving videos, telemedicine, video conferencing, and video monitoring are sometimes exploited enormously. Video streaming in smart phone normally streams visual data from the end user to another. Due to the popularity of this technique, security matters are one of the challenges or vital attributes to be concern. Thus the main focus to be explored include data encryption for video streaming to securing the contents of translated media, which considered as a challenge due to; video streaming requirements, data communications, data retrieval, video contents compression and resource of hardware requirements. Conversely, wireless network communications development leads to transmitting and receiving videos that is captured directly, in the internet technology revolution and embedded systems with usage related to data streaming namely in videos, images, for instance entertainments, personal usages, education, commercial fields, politics and defense. Moreover, for data contents of video streaming, the need to transmit securely to protect sensitive data, from being attacks is crucial since the data have to be protected before sending across the communication network.

Chen Xiao et al.[10] presents, the dissymmetry between massive multimedia data and the limited resources has been studied, and a practical application oriented analytic principle for optimizing encryption of multimedia data has been given; secondly, an all-purpose lightweight speed adjustable video encryption scheme and an improved version are proposed; thirdly, an embedded real-time video sensing system using DSP and ARM has been designed, and the presented encryption schemes have been implemented in data storing and transmission respectively; finally, experimental analyses show the performance of the presented schemes are effective enough to support real-time applications. An all-purpose Speed Adjustable Fast multimedia Encryption scheme (SAFE) will be proposed.

I-Jen Lai et al.[1] proposes a new type of art image, called secret-fragment-visible mosaic image, which contains small fragments of a given source image is proposed in this paper. Observing such a type of mosaic image, one can see all the fragments of the source image, but the fragments are so tiny in size and so random in position that the observer cannot figure out what the source image looks like. Therefore, the source image may be said to be secretly embedded in the resulting mosaic image, though the fragment pieces are all visible to the observer. And this is the reason why the resulting mosaic image is named secret-fragment-visible. a secret image is first divided into rectangular-shaped fragments, called tile images, which are fitted next into a target image selected from a database to create a mosaic image. The number of usable tile images for this operation is limited by the size of the secret image and that of the tile images. This is not the case in traditional mosaic image creation where available tile images for use essentially are unlimited in number because the tile images are not generated from the secret image and may be used repeatedly. Then, the information of tile-image fitting is embedded into some blocks of the mosaic image, which are selected randomly by a secret key. Accordingly, an observer possessing the key can reconstruct the secret image by retrieving the embedded information, while a hacker without the key cannot.

Ya-Lin Lee and Wen-Hsiang Tsai et al. [11] proposes method in which a new type of computer art image, called secret-fragment-visible mosaic image, was used. The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image preselected from a database. But an obvious weakness of Lai and Tsai is the requirement of a large image database so that the generated mosaic image can be sufficiently similar to the selected target image. Using their method, the user is not allowed to select freely his/her favourite image for use as the target image. It is therefore desired in this study to remove this weakness of the method while keeping its merit, that is, it is aimed to design a new method that can transform a secret image into a secret fragment-visible mosaic image of the same size that has the visual appearance of any freely selected target image without the need of a database. In this method, after a target image is selected arbitrarily, the given secret image is first divided into rectangular fragments called tile images, which then are fit into similar blocks in the target image, called target blocks, according to a similarity criterion based on color

variations. Next, the color characteristic of each tile image is transformed to be that of the corresponding target block in the target image, resulting in a mosaic image which looks like the target image. Relevant schemes are also used to conduct nearly lossless recovery of the original secret image from the resulting mosaic image. The method is new in that a meaningful mosaic image is created; in contrast with the image encryption method that only creates meaningless noise images. Also, the existing method can transform a secret image into a disguising mosaic image without compression, while a data hiding method must hide a highly compressed version of the secret image into a cover image when the secret image and the cover image have the same data volume.

III. Proposed Methodology

For secure video transmission, here we use the technique of secret fragment visible mosaic image. MOSAIC is a type of artwork created by composing small pieces of materials, such as stone, glass, tile, etc. Invented in ancient time, they are still used in many applications today. Many methods are proposed to create different type of mosaic images by computer. There are different types of computer mosaic images including, crystallization mosaic, ancient mosaic, photo-mosaic, and puzzle image mosaic. The first two types are obtained from decomposing a source image into tiles (with different colors, sizes, and rotations) and reconstructing the image by properly painting the tiles, and so they both may be called tile mosaics. The other two types of mosaics are obtained by fitting images from a database to cover an assigned source image, and both may be called multi-picture mosaics. The mosaic video is a combination form of different mosaic images (frames). A new type of art image, called secret-fragment-visible mosaic image, which contains small fragments of a given source image is proposed by I-Jen Lai et al.[1] in the year 2011. In such mosaic images, all the fragments of secret/source image can be seen. But the fragments are so tiny in size and randomly arranged the observer cannot find it out. Therefore, the secret image may be said to be secretly embedded in the resulting mosaic image, though the fragment pieces are all visible to the observer. Because of this characteristic of the new mosaic image, it may be used as a carrier of a secret source image in the disguise of another—a target image of a different content. It is useful for the application of covert communication or secure keeping of secret images. More specifically, as illustrated by figure 1, a secret image is first divided into rectangular-shaped fragments, called tile images, which are fitted next into a target image freely selected which creates a mosaic image.

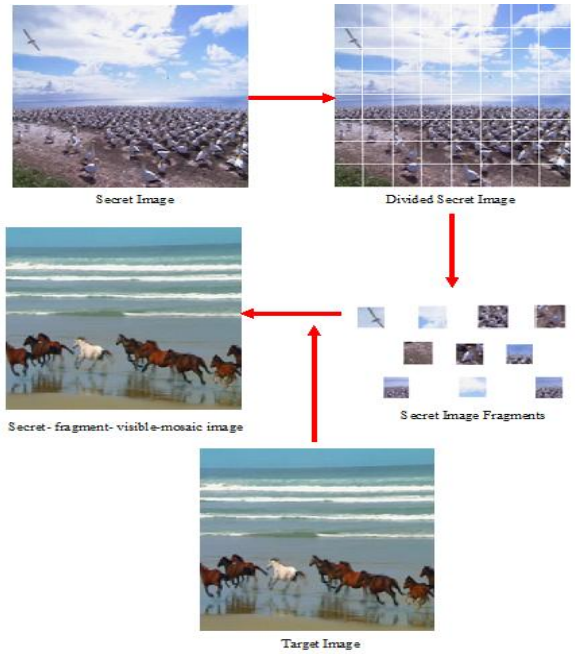


Fig. 1. Creation of secret-fragment-visible mosaic image.

In the proposed method, initially the user can define the number of frames. Then both video segments are converted into frames shown in fig. 2. Then the processing technique is applied in each frame and at last frames are combined to form the mosaic video and reverse process is applied in case of retrieval process.

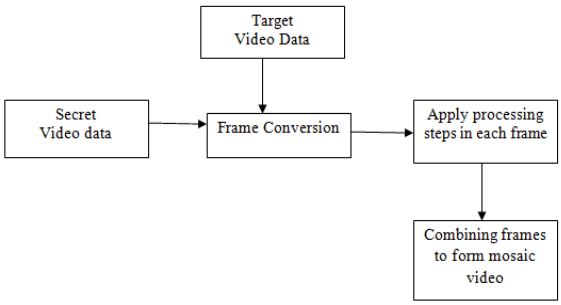


Fig. 2. Functional block diagram of overall process

The proposed system includes mainly two phases shown in figure 3 in 1) mosaic image creation; and 2) secret image recovery. But as an initial work both video segments are converted into frames.

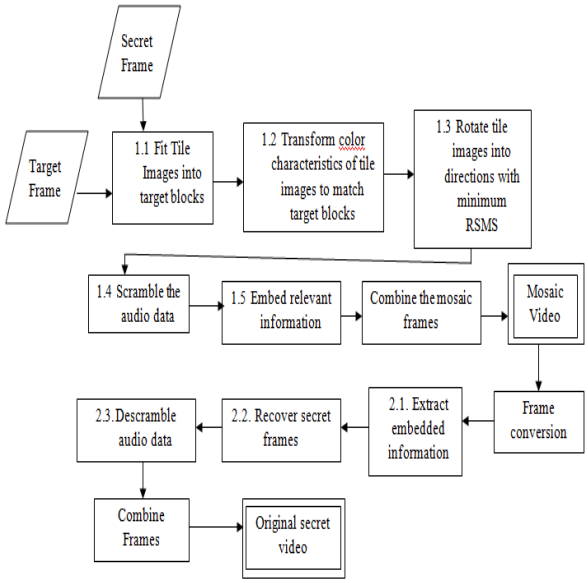


Fig. 3. Functional block diagram

A. Mosaic Image Creation

Initially the user has to select a video data (secret video) that is to be transmitted securely to a receiver. Specifically, after a target video is selected arbitrarily, and then the secret and target video modules are divided into frames. Along with the objects in the module the audio data is also fragmented, with respect to each frame. And the order of audio data sequence is changed and randomly place in different frames. Thus any one can't recognize the actual audio clip from the created mosaic image. In the processing stage, first secret frame is first divided into rectangular fragments called tile images, which then are fit into similar blocks in the target frame, called target blocks, according to a similarity criterion based on colour variations. In the first phase, a mosaic video is yielded, which includes set of frames. The phase includes four stages: 1) Fitting the tile images of the secret frame into the target blocks of a pre-selected frame of a target video; 2) Transforming the color characteristic of each tile image in the secret frame to become that of the corresponding target block in the target frame. Then the color transformation of image is done equation (1).

$$Ci' = qc\ (ci-\mu c)+\mu c \qquad (1)$$

Where, qc is standard deviation of target divided by secret frame, ci is the secret tile, μc is the mean of secret frame, μc' is the mean of the target frame.; 3) Rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block. The blocks are rotated in 0, 90, 180, 270 degrees of angle and the angle with minimum error is selected as the correct position of block. And the block is fixed at that position;

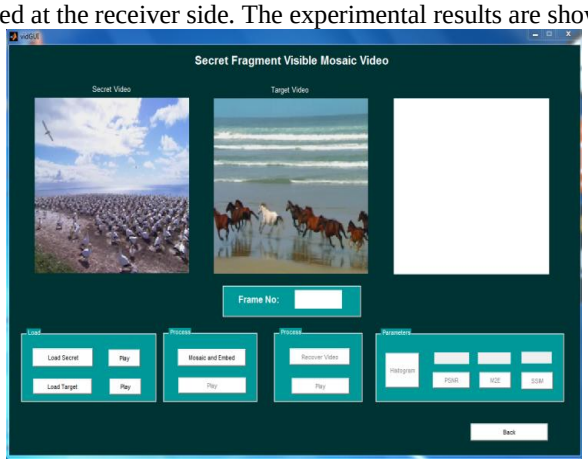
4) scramble the audio data in the video. Then audio data is taken and split according to each frame and randomly place the parts in different frames. And also, sound data of secret video should be embedded inside the mosaic video created, and transmitted along with secret video; 5) embedding relevant information into the created mosaic image for future recovery of the secret video. Huffman encoding is also introduced for the minimization of embedded data. Only by using the key the data is embedded. By using only the same key the secret image is retrieved. Otherwise an error is shown. Then combining these secret frames to form a mosaic video.

B Secret Image Recovery

The reverse process is carried out at the receiver end, first of all the receiver should enter the right key shared by the sender. Then convert the mosaic video into mosaic frames. Using the right key the embedded information should be extracted from each frame. The Huffman decoding uncompresses the data embedded inside each frame. Then reshuffle the blocks to form the original secret frame and does the reverse color transform. Rotate the blocks of embedded mosaic image in reverse direction, in the angle extracted. Then descramble the audio data and combines the frames to form secret video. Thus generates the original secret video at the receiver end.

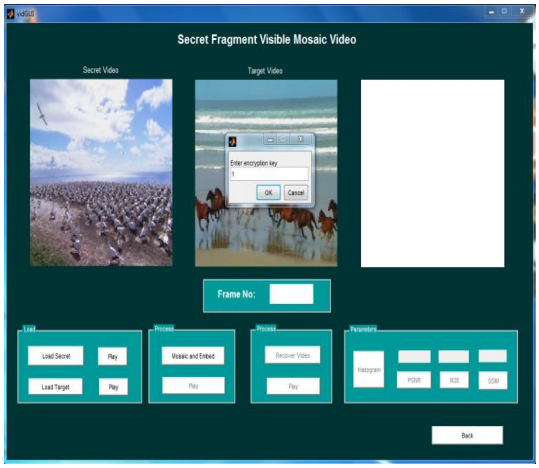
B. Result And Analysis

The proposed system was implemented using the MATLAB and good results are obtained. The secret fragment mosaic video formed will be look like the target video selected for transmission, only small distortion is happened. The data (used for recovery of secret video) embedded mosaic video is also similar to the secret fragment mosaic video. When the user entered key at sender side is similar to the key entered at receiver, then only the original secret video is retrieved. If key entered is wrong, error is happened. As the block size of frames changes the mosaic video clarity changes. Block size is less, clear mosaic video is formed, but needs more time to execute. If the block size of frames is large; clarity of mosaic video is less, only less time needed for processing. Audio data is losslessly recreated at the receiver side. The experimental results are shown in figure 4.

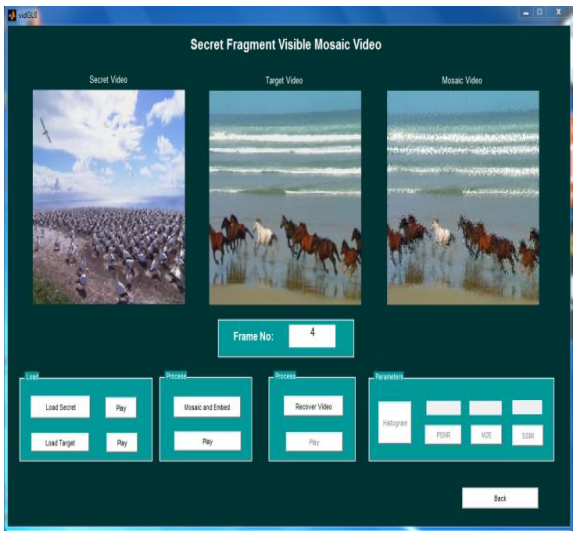


a. Secret and Target video selection

b.



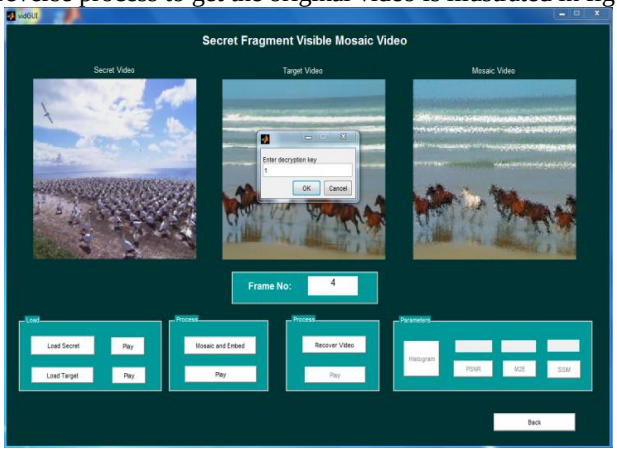
b. Giving encryption key for data embedding



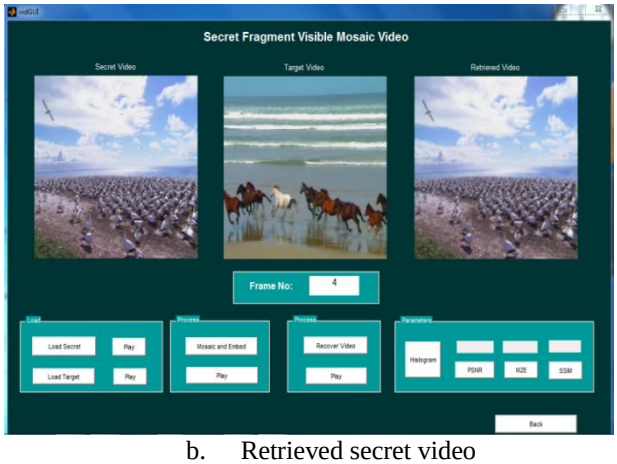
(c) Data embedded mosaic video plays

Fig. 4. Secret-Fragment- Visible Mosaic Image conversion result.

At the receiver side the reverse process to get the original video is illustrated in figure 5.



a. Giving correct key for decryption



b. Retrieved secret video

Fig. 5. Original video extraction at the receiver

Analysis of the results shown in figure 6 actually does a cross checking of the obtained result is whether exact or not. Only by the analysis of the results, we can conclude that the obtained results are valuable for the further studies. The analysis is the only method through which the performance of the system can be measured. By different ways the analysis can be performed. Different types of analysis done here are time analysis and the security analysis.

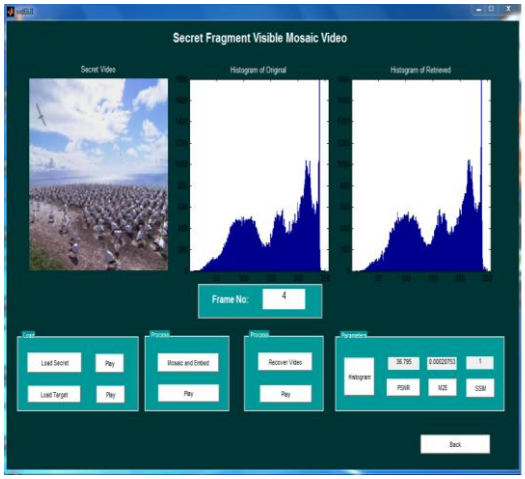


Fig. 6. Analysis of system

Also a relevant parameter is the 'block size'. Block size is the size of each block, when the secret and target frames are divided into different blocks. In the proposed system, when the block size is increases the processing time increases i.e. the speed of execution of the program is high. And when the block size decreases, the speed of execution will decreases. But when the block size is small the quality of the secret fragment mosaic video formed is of good quality. As the block size increases then the quality of mosaic video will decreases. And distortion happens to the mosaic video.

References

[1] I-Jen Lai and Wen-Hsiang Tsai,"] Secret-Fragment-Visible Mosaic Image–A New Computer Art and Its Application to Information Hiding", IEEE transactions on information forensics and security, vol. 6, no. 3, September 2011

[2] Howard Cheng and Xiaobo Li, Senior Member, IEEE, "Partial Encryption of Compressed Images and Videos", IEEE transactions on signal processing, vol. 48, no. 8, august 2000

[3] Zhenfei Zhao and HaoLuo, Zhe-Ming Lu, "Joint Secret Image Sharing and Progressive Transmission Based on Integer Discrete Cosine Transform", 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing

[4] J.K. Mandal#1, S. Ghatak, "Secret Image / Message Transmission through Meaningful Shares using (2, 2) Visual Cryptography (SITMSVC)", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 978-1-4577-0590-8/11/$26.00 ©2011 Ieee Mit, Anna University, Chennai. June 3-5, 2011

[5] Wei-Jen Wang, Cheng-Ta Huang, and Shiuh-Jeng Wang, Member, IEEE, "VQ Applications in Steganographic Data Hiding Upon Multimedia Images", Ieee Systems Journal, Vol. 5, No. 4, December 2011

[6] Shan-Chun Liu and Wen-Hsiang Tsai, Senior Member, IEEE, "Line-Based Cubism-Like Image—A New Type of Art Image and its Application to Lossless Data Hiding", IEEE transactions on information forensics and security, vol. 7, no. 5, october 2012

[7] Kai-Hui Lee and Pei-Ling Chiu, "Digital Image Sharing by Diverse Image Media", IEEE transactions on information forensics and security, vol. 9, no. 1, january 2014

[8] Hirdesh Kumar and AwadheshSrivastava, "A Secret Sharing Scheme for SecureTransmission of Color Images", 978-1-4799-2900-9/14/$31.00 ©2014 IEEE

[9] Mohammed A. Saleh, HabibahHashim, Nooritawati Md. Tahir, "A Low Computational Method of Secure Video Streaming in Mobile System", 2014 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE) , April 7 -8, 2014, Penang, Malaysia

[10] Chen Xiao, Wendong Wang, Nan Yang, "A Video Sensing Oriented Speed Adjustable Fast Multimedia Encryption Scheme and Embedded System", 978-1-4799-4811-6/14/$31.00 ©2014 IEEE

[11] Ya-Lin Lee and Wen-Hsiang Tsai," A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations", IEEE transaction on circuits and system for video technology, vol. 24, no. 4, April 2014.