Secure Image Transmission Using Secret Fragment Visible Mosaic Image In Videos

Divyat L
M-Tech , Computer &Information Science
SIST, Thiruvananthapuram

Ms. Neena Raj N R
Assistant Professor
SIST, Thiruvananthapuram

***Abstract*— A new secure image transition technique through video is proposed, which transforms a given high volume secret image into a SFVM -Secret Fragment Visible Mosaic image of the equal size. The mosaic image looks similar to an arbitrarily selected target image, that is one of the frame of given video. It can be used as a camouflage of the secret image and is produced by dividing the secret image into small parts and transforming their color characteristics to be those of the appropriate blocks of the target image. A technique called secret-fragment-visible mosaic image is used to conduct the color conversion process so that the secret image may be recovered nearly losslessly. The information needed for recovering the secret image is embedded in the video, into the created mosaic image by a lossless data hiding scheme using key. It is mainly focused on to develop a new method for secure image transmission to improve the security and efficiency of image transmission. The proposed method is to show good experimental results.**

Index Terms—Data hiding, Color transformation, image compression, image encryption and decryption, mosaic image, secure image transmission, video technology.

I. INTRODUCTION

In the present world as the information and data become more and more valuable, security is the main problem and protection of that data, which comes from text data to various media types like text, audio, video, and animation. Multimedia data comprise high percentage of images so its protection is very important. This multimedia data protection is done by secret fragment visible mosaic images. There are so many different skillful techniques design to conduct for protection of this secret image from unauthorized access. In today's world where nothing is secure, the security of images is very important. The main area of this work comes under image processing.

Image processing is a method which process the images using mathematical operations .Here the input is an image, such as a photo or video frame and the output may be either an image or a group of characteristics or parameters related to the image. This day, image processing is among rapidly growing technologies. Image processing system includes handling images as two dimensional signals and applying signal processing methods to them. In the natural world ,an image is expressed to be a function of two real variables, for example, f(a, b) with f as the amplitude of the image at the real coordinate position (a, b). Image processing is promptly growing technology with its applications in various aspects of a business. Image Processing is an approach to enhance raw images received from sensors /cameras placed on satellites, area probes or pictures taken in today life for various applications. It forms core research are within engineering and computer science disciplines.

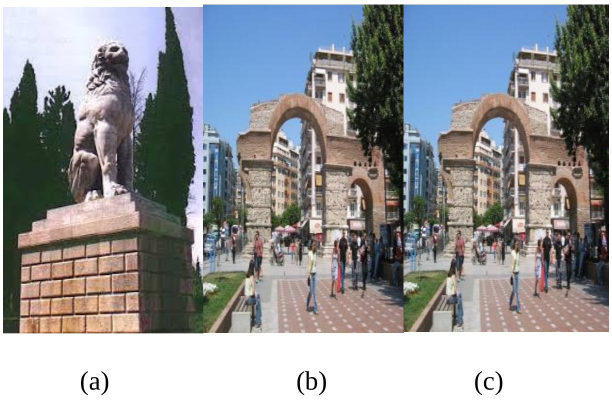
Today, images are frequently transmitted from various sources through the internet for various purposes such as confidential enterprise archives, document storage systems,personal photographs albums, medical imaging systems, and some military image databases. These images usually contain secret or confidential information so that they should be protected from leakages during the secure transmissions. Now, several methods have been proposed for protecting these images from leakage. When an image is transmitted, two common method are applied for secure transmission are image encryption and data hiding.

Image encryption is a technique it convert the original image into another form that is difficult to understand. It is a method that makes use of the natural property of an image, such as high redundancy and strong spatial interrelationship, to get an encrypted image. The encrypted image is a noise image so that no one can access the secret image without knowing decryption of original image that is difficult to understand. The encrypted image is a noise image so that no one can access the secret image without knowing a decryption key. In corporate world,the main application of image encryption is health care, military operation, and multimedia systems. An encrypted image is a useless file until it is decrypted and due to its randomness, it may also stimulate an attacker's attention by transmission.

To overcome this problem, data hiding that hides a secret message into a target image so no one can understand the existence of the secret data. A main issue of hiding data in images is the difficulty to embed a huge amount of message data into a single image. Especially, if one wants to hide a secret image into a target image with equal size, the secret image must be highly compressed in previously. But, so many applications such as transmitting medical images, military images, permissible documents, etc., that are valuable with no contribution of gloomy distortion, such data compression operations are usually impossible.

To overcome these problem a secure image transmission technique using secret fragment visible mosaic images is developed, which automatically transform a given large - volume secret image into secret fragment visible mosaic image of the equal size. The mosaic image, which looks similar to a swiftly selected target image and may be used as a camouflage of the secret image, i produced by dividing the secret image into small parts and converting their color characteristics to be those of the equivalent blocks of the target image. The size of the mosaic image is a main problem in the time of embedding. The compressed and encrypted structure are embedded into the mosaic image, the size of the mosaic image is limited. So some information may be lost and security is decreased.

To overcome this problem, a new technique for secure image transmission using secret fragment visible mosaic image through video is proposed, which translates a secret image into a meaningful mosaic image with the same size and which looks like a selected target image of the available video frames.



(a) Secret image. (b) Cover image. (c) Secret-fragment-visible mosaic image created from (a) and (b)

Fig. 1.1 Secret Fragment Visible Mosaic Image Creation

Specifically, after a target image is selected immediately, the given secret image is first divided into rectangular fragments called tile images, which then are embed into similar blocks in the target image, called target blocks, according to a similarity benchmark based on color variations. Next, the color characteristic of each tile image is transformed to be that of the equivalent target block in the target image, resulting in a mosaic image which looks like the target image. Related schemes are also proposed to conduct nearly lossless recovery of the original secret image from the resulting mosaic image.

II. LITERATURE SURVEY

Ya-Lin Lee and Wen-Hsiang Tsai [1], presented a new secure image transmission technique via secret-fragment-visible mosaic images. In this paper Ya-Lin Lee shows a technique for the transmission of the secret image securely and losslessly. This method converts the secret image into a mosaic tile image having the same size of the target image which is selected from a database. This color transformation is controlled and the secret image is recovered losslessly from the mosaic tile image with the help of the extracted information generated for the recovery of the image. The secret image and the target image are selected outside the use of database and without any restrictions on the selections. The drawback of this paper is that it cannot be applied to the images of other color models other than RGB and the size of the available target images should be small size than secret image then created mosaic image is become blurred. The size of the mosaic image is a main problem in the time of embedding. The compressed and encrypted structure are embedded into the mosaic image, the size of the mosaic image is limited. So some information may be lost and security is decreased.

Pratibha S Ghode, Prof. Pragati Patil, Prof. Vinod Nayyar, Prof. Shashank Moghe [2] presented a keyless approach to image encryption. This paper shows a keyless approach to encryption methods which are used to encrypt images. This is done by generating appropriate information with the help of some RMSE value which helps to rotate the tile images to a certain angle. The procedure of encryption and decryption implemented considered being having better security using SST methods without using any key. In this methods at improving the level of security and secrecy provided by the digital color image encryption. The image encryption and decryption algorithm is designed and implemented to provide confidentiality and security in transmission of the image. The encryption algorithm can ensure the lossless of transmissions of image. An approach to implement keyless access to lossless image encryption of the every pixel of image and encrypted them.

Ashwind S, Ganesh K, Gokul R, Ranjeeth Kumar C, presented secure data transmission using reversible data hiding. In this Paper [3], a method that can achieve real reversibility i.e., data extraction and image recovery are free of any error. Their experiments show that this method can embed more data for the same image quality,such as for PSNR = 40 db. More and more interest is paid to reversible data hiding (RDH) in encrypted images, since it maintains the good property that the original image can be losslessly recovered after embedded data is extracted while protecting the image content’s privacy. Unlike previous methods.The method can achieve real reversibility i.e., data extraction and image recovery are free of any error.

Rucha R Raut, Prof. Komal B Bijwe [4], mentioned aboutvisual cryptography and secret fragment visible mosaic images. In this paper, they had done the literature survey on existing work which used different techniques for image hiding from 2001 to 2014 and also given common introduction about visual cryptography and secret fragment visible mosaic images. Good mosaic image creation outcomes are guaranteed only when the database is large in size so that the selected target image can be sufficiently identical to the input secret image.

The main objective of the proposed system is to provide more secure and efficient transmission method for image transmission. A technique in which a secret image is transformed into a useful mosaic image of the same size .The mosaic image is similar to target image. This transformation process is controlled by a secret key using which receiver can recover the secret image. This technique is called secret-fragment-visible mosaic image.

III .IDEAS OF THE PROPOSED METHOD

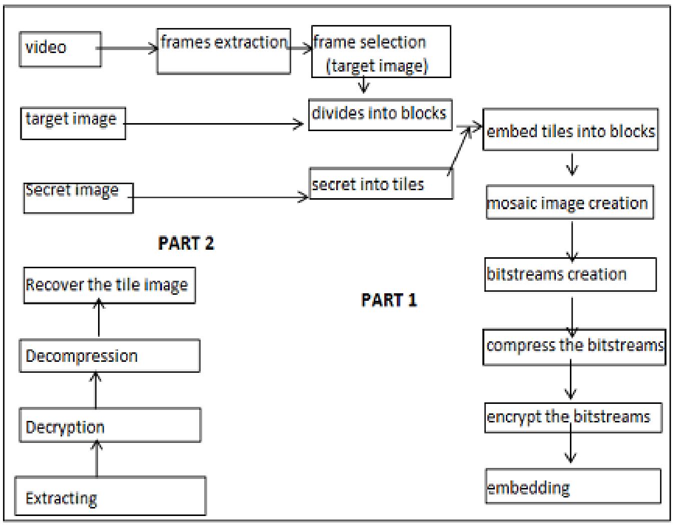


Fig.2.Flow diagram of the proposed method.

The above block diagram consists of two parts: Mosaic image creation and secret image recovery.

A. MOSAIC IMAGE CREATION

In this first phase,which a secret image is divided into different parts.Now fitting the tile images of the secret image into the target blocks of a target image.The target image is one of the frame from video or a normal image .After this translating the color characteristic of each tile image in the secret image to become that of the equivalent target block in the target image and rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding cover block.After the rotation embedding appropriate information into the created mosaic image for future restoration of the secret image .In this way to get the output secret fragment visible mosaic image.

Algorithm 1 : Mosaic Image Creation

Input: a secret image S, a cover image T, and a secret key K.
Output: a secret-fragment-visible mosaic image F.
Steps:
Step 1: Check the size of the secret image and target image. If the size are not equal then change to be identical and dividing the secret image into n tile images $\{T_1, T_2, ..., T_n\}$ as well as target into n target blocks$\{B_1, B_2, ..., B_n\}$.

Step 2: Calculate the mean and standard deviation of each tile image $T_i$and each target blocks $B_j$for three color channel.

Step 3: Calculate the average standard deviations for T_i and B_j, respectively, for i = 1 through n and j = 1 through n.

Step 4 : Sort the tile images in the set $S_{tile} = \{T_1, T_2, ...,T_n\}$ and the target blocks in the set $S_{target} = \{B_1, B_2, ... , B_n\}$ according to the obtained average standard deviation values of the blocks;

Step 5: Maps the blocks in the sorted S_{tile} to the sorted S_{target} in a one to one manner; and reorder the mappings according to the indices of the tile images,

Step 6:Create a mosaic image F by fitting the tile images into the corresponding target blocks.

Step7. Set up a counting table TB with 256 entries, each with an index corresponding to a residual value.

Step8. For each mapping $T_i \rightarrow B_{ji}$ represent the means μ_c and μ^{1}_{c} of T_i and B_{ji}, respectively, by eight bits; and perform the standard deviation quotient q_c where c = r, g, or b.

Step 9.For each pixel(p_i) in each tile image (T_i) of mosaic image F with a color value (c_i) where c = r, g, or b, transform ci into a new value c_i^{11}, if c_i^{11} is not less than 255 or if ci^{11} is not greater than 0, then change c_i^{11} to be 255 or 0, respectively; Calculate a residual value R_i for pixel pi.

Step 10.Calculate the RMSE values of each color transformed tile image Ti in F with respect to its appropriate target block B_{ji} after rotating Ti into every of the directions $\theta = 0^o$, 90^o,180^o and 270^o.

Step 11.Rotate T_i into the optimal direction $\theta^o$with the smallest RMSE value.

Step 12.Construct a Huffman table HT by the content of the counting table TB to encode all the residual values computed previously.

Step13. For each tile image T_i in mosaic image F, form a bit stream M_i for recovering T_i.

Step14. Concatenate the bit streams M_i of all T_i in F in a raster-scan order to form a total bit stream M_t; the secret key K is used to encrypt Mt into another bit stream M_t^1; and embed M_t^1 into F by the reversible contrast mapping scheme.

Step15. Construct a bit stream I involves the number of conducted iterations Ni for embedding M_t^1; the number of pixel pairs N pair used in the final iteration; and the Huffman table HT constructed for the residuals; and embed the bit stream I into mosaic image F by the related scheme used in Step 13.

B. SECRET IMAGE RECOVERY

In this second part, extracting the embedded information from the mosaic image for secret image recovery. The secret image is recovered by using the extracted information by secret image recovery algorithm. In this phase result will be calculated and to make perfect if required result is in the form of delay and accuracy.

Algorithm 2: Secret Image Recovery

Input: a mosaic image F with n tile images $\{T_1, T_2,...,T_n\}$ and the secret key K.

Output: the secret image S.

Steps:
Step 1.Extract the bit stream I from F and decode it.
Step 2.Extract the bit stream M_t^1 using the values of N_i and N_{pair}.
Step3. Decrypt the bit stream M_t^1 into M_t by K.
Step 4.Decompose Mt into n bit streams M1 through M_n for then to-be-constructed tile images T_1 through $T_n$in S, respectively.
Step 5.Decode M_i for each tile image T_i.
Step 6.Recover 1 to 1 in a raster-scan order the tile images T_i, i = 1 through n, of the desired secret image S
Step 7.The desired secret image S is the output by composing all final tile images.

IV. CONCLUSION

To developed a secure and efficient method for image transmission using secret fragment visible mosaic image in videos. Good experimental results shown to the feasibility of the proposed method. Future studies may be to applying the proposed method to image of color models other than the RGB.

REFERENCES

[1] Ya-Lin Lee, Student Member, IEEE, and Wen-Hsiang Tsai, Senior Member, IEEE in "A New Secure Image Transmission Technique via Secret-fragment-Visible Mosaic Images by Nearly Reversible Color Transformations",IEEE Transactions On Circuits And Systems For Video Technology, vol.24[2014].

[2] Pratibha S.Ghode , Prof. PragatiPatil, Prof. Vinod Nayyar, Prof.Shashank Moghe, "A Keyless Approach to Image Encryption", International Journal of Innovative Research in Advanced Engineering (IJIRAE), vol. 4[2014].

[3] Ashwind S, Ganesh K, Gokul Rand Ranjeeth Kumar ,"Secure DataTransmission Using Reversible Data Hiding" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5[2014]

[4] Rucha R. Raut and Prof. KomalB.Bijwe , "A Survey Report on Visual Cryptography and Secret Fragment Visible Mosaic Images"International Journal of Application or Innovation in Engineering & Management(IJAIEM),vol.3[2014].

[5] Pragati Pal and Sukanya Kulkarni , "Data Hiding based on Color Image Compression Technique"International Journal of Computer Applications (09758887)International Conference and Workshop on Emerging Trends in Technology vol.5 [2014].

[6] Kede Ma, Weiming Zhang, Xianfeng Zhao, Member IEEE, Nenghai Yu, and Fenghua Li ,"Reversible Data Hiding in Encrypted ImagesbyReserving Room before Encryption",IEEE Signal Processing,vol.15[2007].

[7] I.J Lai and W.H Tsai, "Secret- Fragment-Visible Mosaic Image- A New Computer Arts and its Applications to information Hiding", IEEE Transactions On Information Forensics And Security,vol. 6[2011].

[8] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSBsubstitution", IEEE Transaction in Forens.,vol.37[2004]

[9] [9] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform, "IEEE Trans. Inf. Forens. Secur.,vol. 2, [2007].

[10] Ragasudha R and Sampathkumar K, "Mosaic Image Creation & Transmission Technique Based on CMYK" ,International Journal Of Innovative Research In Science, Engineering And Technology9(IJITET) ,vol.4[2015]