ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

Mosaic Image Creation in Videos for Secure Image Transmission

S.Pragatheeswari[1], Maram Reddy Srija[2], Mannuru Tejaswini[3], M.S.Vinmathi M[4].

Department of CSE, Panimalar Engineering College, Chennai, India[1,2,3]

Associate Professor, Department of CSE, Panimalar Engineering College, Chennai, India[4]

ABSTRACT*:* A new secure image transmission technique through videos is proposed, which transforms a given large-volume secret image into a secret-fragment-visible mosaic image of the same size. The mosaic image looks similar to an arbitrarily selected target image, which is one of the frames of the given video. It can be used as a camouflage of the secret image and is yielded by dividing the secret image into fragments and transforming their color characteristics to be those of the corresponding blocks of the target image. A technique called secret-fragment-visible mosaic image is used to conduct the color transformation process so that the secret image maybe recovered nearly losslessly. The information required for recovering the secret image is embedded in the video, into the created mosaic image by a lossless data hiding scheme using a key. The proposed method is known to show good experimental results**.**

KEYWORDS: Color transformation, data hiding ,image encryption, mosaic image, secure image transmission, video technology.

I. INTRODUCTION

In recent times, images from various sources are sent and received over the internet for various applications, such as online confidential enterprise archives, document storages, medical image databases, and military imaging systems. The images usually contain confidential information i.e they should be protected from leakages and attacks during transmissions. Various methods have been proposed for secure image transmission, in which there are two common approaches- image encryption and data hiding. Image encryption is a technique in which the natural property of an image like high redundancy and strong spatial correlation, to get an image encrypted based on Shannon's confusion and diffusion properties [1]–[7] are used. The resultant image is just a noiseful file that no one can understand or obtain the secret image from it unless has the correct key. But, the encrypted image is a meaningless, noiseful image, which is totally unusable before decryption and may arouse an attacker's attention during transmission because of its randomness and chaotic form . Another aspect of information security data hiding [8] that hides a secret image into a cover image so that it is hard to realize the existence of the secret data. The data type of the secret message discussed in this paper is an image. Existing methods mainly make use of the techniques of LSB substitution [8], histogram shifting, difference expansion, prediction-error expansion, recursive histogram modification, and discrete cosine/wavelet transformations.. A main drawback of the methods for data hiding is that there is difficulty in embedding a large amount of message into a single image. Also, if one wants to hide a secret image into a cover image with the same size, the image must be highly compressed before usage. . However, for many applications, such as transmission of medical pictures, military images, legal documents, etc., that are valuable with no possiblity of serious distortions, such as data compression operations are usually impractical. In this paper, a new technique for secure image transmission through videos is proposed, which transforms a secret image into a meaningful mosaic image with the same size and which looks like a preselected target image of the available video frames. The process is controlled by a secret key for security. This key has to be used by the person in order to recover the secret image losslessly from the video otherwise called as target image.

II. EXISTING WORK

The existing method is quoted by Lai and Tsai, in which a called secret-fragment-visible mosaic image was proposed. It is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image which is selected priorly from a database. The drawback of Lai and Tsai is that it requires a large image database so

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

that the created mosaic image appropriately resembles the selected target image. In this, the user is not allowed to select freely his/her favorite image for use as the target image. Hence, to remove this weakness of the above method while retaining its advantage, which is aimed to develop a new method that can transform a secret image into a same sized secret fragment-

Fig.1. Result yielded by the proposed method.(a)Secret image.(b)Target image.(c)Secret-fragment-visible mosaic image created from(a)and(b)by the proposed method.

III. PROPOSED WORK

As an illustration, Fig. 1 shows a result yielded by the proposed method. Specifically, after a video frame is selected arbitrarily, the given secret image is first divided into rectangular fragments called tiles, which then are fit into similar blocks in the target image, called blocks(target), based on a similarity criteria of color variations. Also, the color characteristic of each tile is transformed to the color characteristic of the corresponding target block of the above said target image.It forms a mosaic image which looks like the target image. Similar methods are also proposed to perform close-to lossless recovery of the original image from the resulting image. The proposed method is new where in a meaningful image is created, where as in the image encryption method only meaningless images are created .Moreover, this method can transform a secret image into a disguising image without compression, while a data hiding method should hide a highly compressed image into a mosaic image when the secret image and the cover image have the same data size.

IV. 4.MODULE DESCRIPTION:

4.1. Upload Video and Secret Image.

Here, the user is supposed to login as an admin. The user can select any video and upload it. It is followed by Decompressing the video frames into 800x800 pixels format. After obtaining all frames from the video (10f per seconds), the frames are saved in a databas and later used for reference while selecting a target image. Also the user is required to upload any one secret image depending upon the likes of the user.

4. 2. Color transformation and Computation.

Here, the user selects a secret image and target image then split into 4x4 matrixes of Tile images. We need to compute the entire tiles pixels and features for further color transformations. If the size of the target image B is different from that of the secret image A, change the size of B to be identical to that of A; and divide the secret image A into n tile images {T1, T2, . . . , Tn} as well as the target image B into n target blocks {B1, B2, . . . , Bn} with each Ti or Bi being of size NT. Compute the means and the standard deviations of each tile image Ti and each target block Bj for the three color channels ; and compute accordingly the average standard deviations for Ti and Bj , respectively, for i = 1 through n and j = 1 through n. Sort the tile images in the set Stile = {T1, T2, . . . , Tn} and the target blocks in the set A target = {B1, B2, . . . , Bn} according to the computed average standard deviation values of the blocks; map in order the blocks in the sorted Stile to those in the sorted A target in a 1-to-1 manner; and reorder the mappings according to the indices

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

of the tils, resulting in a mapping pattern(sequence) L of the form: T1 → Bj1 , T2 → Bj2 , . . . , Tn → Bjn .

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i, \quad \mu_c{}' = \frac{1}{n}\sum_{i=1}^{n} c_i{}' \qquad (1)$$

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i - \mu_c)^2}, \quad \sigma_c{}' = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i{}' - \mu_c{}')^2} \qquad (2)$$

in which c_i and c_i' denote the C-channel values of pixels p_i and p_i', respectively, with $c = r$, g, or b and C = R, G, or B. Next, we compute new color values (r_i'', g_i'', b_i'') for each p_i in T by

$$c_i{}'' = q_c(c_i - \mu_c) + \mu_c{}', \qquad (3)$$

in which $q_c = \sigma_c'/\sigma_c$ is the standard deviation quotient and $c = r$,

Create a mosaic image M by fitting the tile images into the corresponding target blocks according to L. Performing color conversions between the tile images and the target blocks. Create a counting table TB of 256 records, each with an index corresponding to a residual data-value, and assign an initial value of zero to each entry (note that each residual value will be in the range of 0 to 255). For each mapping Ti →Bji in sequence L, represent the means μc and μ _ c of Ti and Bji, respectively, by eight bits; and represent the standard deviation

quotient qc appearing in (3) by seven bits, where c = r, g, or b.

$$c_i = (1/q_c)(c_i{}'' - \mu_c{}') + \mu_c. \qquad (4)$$

For every pixel pi in every tile Ti of mosaic image M with color value ci where c = r, g, or b, transform ci into a new value c__ i by (3); if c__ i is not smaller than 255 or if it is not larger than 0, then change c__ i to be 255 or 0, respectively; compute a residual value Ri for pixel pi ; and increment by 1 the count in the entry in the counting table TB whose index is identical to Ri. For rotating the tile images, here compute the RMSE values of each color transformed tile image Ti in M with respect to its corresponding target block Bji after rotating Ti into each of the directions θ =0, 90, 180 and 270; and rotate Ti into the optimal direction θ with the smallest RMSE value.

$$x' = 2x - y, \quad y' = 2y - x \qquad (6)$$

$$x = \left\lceil \frac{2}{3}x' + \frac{1}{3}y' \right\rceil, \quad y = \left\lceil \frac{1}{3}x' + \frac{2}{3}y' \right\rceil. \qquad (7)$$

4. 3. Create mosaic image and Re-build video.

Construct a Huffman table HT using the content of the counting table TB to encode all the residual values computed previously. For each tile image Ti in mosaic image M, construct a bit stream Mi for recovering Tn, including the bit-segments which encode the data items of: 1) the index of the corresponding target block Bji; 2) the optimal rotation angle θ° of Ti; 3) the means of Ti and Bji and the related standard deviation quotients of all three color channels; and 4) the bit sequence for overflows / underflows with residuals in Ti encoded by the Huffman table HT constructed. Concatenate the bit streams Mi of all Ti in M in a raster-scan order to form a total bit stream Mt; use the secret key K to encrypt Mt into another bit stream M_ t ; and embed M_ t into M by the reversible contrast mapping scheme proposed . Construct a bit stream I including: 1) the number of conducted iterations Ni for embedding M_ t; 2) the number of pixel pairs Npair used in the last iteration; and 3) the Huffman table HT constructed for the residuals; and embed the bit stream I into mosaic image M. Finally getting a mosaic image and Insert into the all target frames. Merge all the frames and build video in *.avi format for uncompressing images.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

4. 4. . Secret images recover from video.

Users upload a video which has the mosaic image. Extract all the frames from video files. And recover all secret image tiles from mosaic image as mentioned given following steps .

4.4.1. Extracting the secret image recovery information.

Extract from M the bit stream I by a reverse version of the scheme proposed in [24] and decode them to obtain the following data items: 1) the number of iterations Ni for embedding M_ t ; 2) the total number of used pixel pairs Npair in the last iteration; and 3) the Huffman table HT for encoding the values of the residuals of the overflows or underflows. Extract the bit stream M_ t using the values of Ni and Npair by the same scheme used in the last step. Decrypt the bit stream M_ t into Mt by K. Decompose Mt into n bit streams M1 through Mn for the n to-be-constructed tile images T1 through Tn in A, respectively. Decode Mi for each tile image Ti to obtain the following data items: 1) the index ji of the block Bji in M corresponding to Ti; 2) the optimal rotation angle θ° of Ti; 3) the means of Ti and Bji and the related standard deviation quotients of all color channels; and 4) the overflow/underflow residual values in Ti decoded by the Huffman table HT.

4.4.2. Recovering the secret image.

Recover one by one in a raster-scan order the tile images Ti, i = 1 through n, of the desired secret image A by the following steps: 1) rotate in the reverse direction the block indexed by ji, namely Bji, in M through the optimal angle θ° and fit the resulting block content into Ti to form an initial tile image Ti; 2) use the extracted means and related standard deviation quotients to recover the original pixel values in Ti 3) use the extracted means, standard deviation quotients, and (5) to compute the two parameters cS and cL; 4) scan Ti to find out pixels with values 255 or 0 which indicate that overflows or underflows, respectively, have occurred there; 5) add respectively the values cS or cL to the corresponding residual values of the found pixels; and 6) take the results as the final pixel values, resulting in a final tile image Ti. Compose all the final tile images to form the desired secret image A as output.

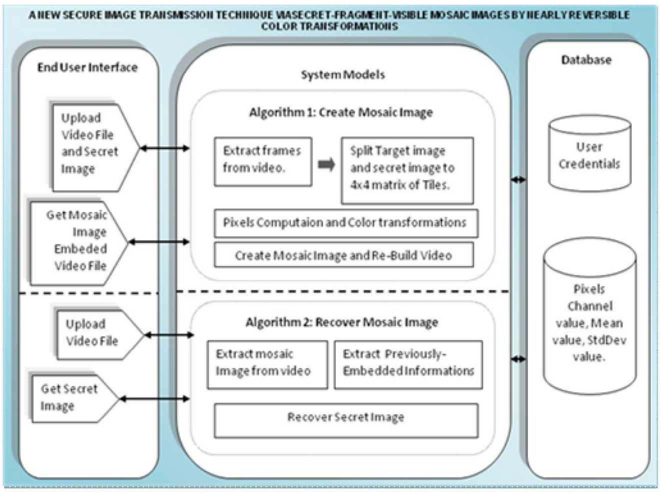

Fig.2. Flow diagram of the proposed method visible mosaic one that has the visual resemblance of any arbitrarily selected target image without the use of an image database.

V. ALGORITHMS OF THE PROPOSED METHOD

Based on the previous discussions, the precise algorithms for mosaic image creation and secret image recovery are provided respectively as Algorithms 1 and 2.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

Algorithm 1:

Mosaic image creation **Input**: a secret image A, a target image B, and a secret key C. **Output**: a secret-fragment-visible mosaic image M.

Steps: **Stage 1. fitting the tile images into the target blocks.**

Step 1. If the size of the target image B is different from that of the secret image A, change the size of Target image to be identical to size of Secret image; and divide the secret image A into n tiles{T1, T2, ..., Tn}and the target image B into n blocks {B1, B2, ..., Bn} with each Ti and Bi with same size NT.
Step 2. Compute the means and the standard deviations of each tile image Ti and each target block Bj for the three color channels according to (1) and (2); and compute accordingly the average standard deviations for Ti and Bj, respectively, for i= 1 through n and j= 1 through n.
Step 3.Sort the tile images in the set Stile ={T1, T2, ...,Tn} and the target blocks in the set A target ={B1, B2, ..., Bn} according to the computed average SD values of the blocks; map the blocks onto the sorted Stile to those in the sorted A target in an one to one manner; and shuffle the mappings according to the indices of the tiles, thus obtaining a mapping sequence L of the form:T1 →Bj1, T2 →Bj2, ..., Tn →Bjn.
Step 4. Create a mosaic image M by fitting the tile images into the respective target blocks according to L.

Stage 2. Performing color conversions between the tile images and the target blocks.

Step 5. Create accounting table TB with 256 entries, each with an index corresponding to residual value, and an initial value of zero to each entry is assigned (note that each residual value will be in the range of 0 to 255).
Step 6. For each mapping Ti →Bji in sequence L, represent the means μc of Ti and Bji, respectively, by 8 bits; and represent the standard deviation quotient tqc appearing in (3) by 7 bits, according to the scheme where c=r, g, or b.
Step 7. For each pixel pi in each tile image Ti of mosaic image M with color value ci where c=r, g,or b, transform ci into a new value ci by (3); if ci is not smaller than 255 or if it is not greater than 0, then change ci to be 255 or 0, respectively; compute a residual value Ri for pixel pi by the way described and increment the count by 1 in the entry in the table TB whose index is identical to Ri.

Stage 3. rotating the tile images.

Step 8. Compute the RMSE values of each color transformed tile image Ti in M with respect to its corresponding block Bji after rotation of tile Ti into each of the directions; and rotate Ti into the optimal direction θ with the smallest RMSE value.

Stage 4. embedding the secret image recovery information.

Step 9. Construct a Huffman table HT using the content of the counting table TB to encode all the residual values computed previously.
Step 10. For each tile image Ti in mosaic image M, construct a bit stream Mi for recovering Ti including the bit-segments which encode the data items of:
1) the index of the corresponding target block Bji;
2) the optimal rotation angle θ° of Ti;
3) the means of Ti and Bji and the related standard deviation quotients of all three RGB color channels; and
4) the overflow/underflow bit sequence with residuals in Ti encoded by the Huffman table HT constructed in the above step.
Step 11. Concatenate the bit streams Mi of all Ti in Fin a raster-scan order to form a total bit stream Mt; use the secret key K to encrypt Mt into another bit Stream Mt; and embed Mt into M by the reversible contrast mapping scheme proposed.
Step 12. Construct a bit stream I including: 1) the number of conducted iterations Ni for embedding Mt;2)the number of pixel pairs N pair used in the last iteration; and 3) the Huffman table HT constructed for the residuals; and embed the bit stream I into mosaic image M by the same scheme used in the previous step.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

Algorithm 2:Secret image recovery

Input: a mosaic image M with n tile images {T1, T2, ...,Tn}and the secret key K.
Output: the secret image A. Steps: ***Stage 1. extracting the secret image recovery information.***
Step 1. Extract from M the bit stream I by a reverse version of the scheme proposed and decode them to obtain the following data items:
1) the number of iterations Ni for embedding Mt; 2) the total number of used pixel pairs N pairing the last iteration; and 3)the Huffman table for embedding the overflow or underflow values of the residuals.
Step 2. Extract the bit stream Mt using the values of Ni and N pair by the same scheme used in the last step.
Step 3. Decrypt the bit stream Mt into Mt byK.
Step 4. Decompose Mt into n bit streamsM1 through Mn for the n to-be-constructed tile images T1 through Tn in A, respectively. Step 5. Decode Mi for each tile image Ti to obtain the following data items:
1) the index ji of the block Bji in M corresponding toTi;
2) the optimal rotation angle θ° of Ti;
3) the means of Ti and Bji and the related SD values of all three RGB color channels; and
4) the overflow/underflow residual values in Ti decoded by the Huffman table HT.

Stage 2. recovering the secret image.

Step 6. Recover one by one in a raster-scan order the tile images Ti, i= 1 through n, of the desired secret image A by the following steps:
1) rotate in the reverse direction the block indexed by ji, namely Bji, in M through the optimal angle θ° and fit the resulting block content into Ti to form an initial tile image Ti;
2) use the extracted means and related SD values to recover the encrypted pixel values in Ti according to (4);
3) use the extracted means, standard deviation quotients, and
(5) to compute the two parameters cS and cL
4) scan Ti to find out pixels with values 255 or 0 which indicate that overflows or underflows, respectively, have occurred there; 5) add respectively the values cS or cL to the corresponding residual values of the found pixels; and 6) take the results as the final values for pixels and hence forming a final tile image Ti. Step 7. Compose all the final tile images to form the desired secret image A as output. Quality metric of root mean square error (RMSE) is utilized, which is defined as the square root of the mean square difference between the pixel values of the two images. A potential drawback of the proposed method is that the volume of available target images should match those of possible input secret images. In precise note, if we have a very secret image which is of large size but a target image which is of relatively small size for selections, then the selected target image should be enlarged before mosaic image creation in order to match the size of the secret image, or else the created mosaic image will become blurred

VI. CONCLUSION

A new secure image transmission through videos has been proposed, which can not only can create meaningful mosaic images but also can transform a secret image into a mosaic of same data size to be used as a camouflage of the secret image. With proper pixel color transformations and skillful schemes for handling overflow, underflow conditions in the conversion values of the pixel colors, secret-fragment visible mosaic images with very close similarities to arbitrarily-considered target images can be created with no need of a large image database. Moreover there is lossless recovery of the original secret images from the created mosaic images. Experimental results have shown great feasibility of the proposed method. Future studies may be one for applying the proposed method to other color models excluding RGB.

REFERENCES

[1] J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps,”Int. J. Bifurcat. Chaos, vol. 8, no. 6,pp.1259–1284, 1998.
[2] G. Chen,Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” Chaos Solit. Fract., vol. 21,no. 3, pp. 749–761, 2004.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

[3] L. H. Zhang, X. F. Liao, and X. B. Wang, "An image encryption approach based on chaotic maps," Chaos Solit. Fract., vol. 24, no. 3, pp. 759–765, 2005.
[4] H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation,"Chaos Solit. Fract., vol. 32, no. 4, pp. 1518–1529, 2007.
[5] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," Chaos Solit. Fract., vol. 35, no. 2, pp. 408–419, 2008.
[6] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaosbased image encryption algorithm,"Chaos Solit. Fract., vol. 40, no. 5,pp. 2191–2199, 2009.
[7] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutationsubstitution scheme for image encryption," Opt. Commun., vol. 284,no. 19, pp. 4331–4339, 2011.
[8] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution,"Pattern Recognit.., vol. 37, pp. 469–474, Mar. 2004.