IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 2, Ver. I (Mar - Apr. 2014), PP 41-45
www.iosrjournals.org

Triple Key Chaotic Encryption And Secret Sharing-Based Method For Authentication Of Color Document Images Via The Use Of The Png Image With A Data Repair Capability

Anu john[1], C. Manjula[2]
1- M.E, Communication System student, Department of Electronics and Communication Engineering
2- Assistant Professor, Department of Electronics and Communication Engineering Adhiyamaan College, Hosur.

Abstract: *In this paper for improving the security of data transmission we are introducing triple key chaotic encryption technique .In addition to this authentication method based on secret sharing technique with a data repair capability is being introduced. Using Shamir secret sharing scheme shares arebeing created from the authentication signal generated for each block of document image alongwith the binarized block content As many shares as possible are generated by properly choosing the involved parameters.PNG image is formed by combiningalpha channel plane with original image.To yield atransparent stego image the computed share values are mapped in to a range of alpha channel values near to their maximum value of 255 during the embedding process.authentication of the document image can be changed by an intruder by superimposing ,painting or adding noise to the image.image is marked as tampered if there is a mismatch between the authentication signal of the current block and that extracted from the shares embedded in alpha channel plane.reparing of data is being done by applying reverse Shamir scheme by collecting shares from the unmarked block.*

Keywords: *Atuthentication,Secret sharing,Encryption*

I. Introduction

Security is the main concern in today's world and securing data from unauthorized access is very important. Different techniques should be used to protect confidential image data from unauthorized access as each type of data has its own features.Image can be defined as an array or a matrix of square pixels arranged in columns and rows.A normal grayscale image has 8 bit colour depth =256 greyscale.A" true colour "image has 24 bit colour depth = 8×8×8=256×256×256 colours=~16 million colours.Encryption is defined as the process of encoding messages in a way that only authorized parties can read it.Encryption is being done using encryption key ,but it doesn't prevent hacking.In the proposed work encryption introduced enhances the security of data.By using the authentication signal generated at the transmitter side any tampering done by the hacker is being identified and it is repaired.

II. System Model

The original document image I is first binarized using Jarvis halftoning technique.This will result in the binarized version of the original image denoted as I_b.Halftoning is a representation technique to transform original image in to continous tone digital image in to binary image of 1's and 0's only.The dta required for authentication and repairing are being computed from this binarzed image.The data computed is taken as input to the shamir's secret sharing scheme[7] for generating the partial shares.These secret shares are embedded in to the alpha channel plane.This stego image obtained is then encrypted using triple key chaotic encryption method for enhancing the security of data transmission.Since the data for authentication and reparing are carried by the alpha channel there is no chance for the destruction of the input image.But conventional authentication schemes sacrifices a part of image contents to accommodate data for authentication purpose.After the data is being transmitted authentication process including the verification and self reparing is done at the receiver.Intially the stego image is being decrypted.Then the authentication data of the current image is calculated and compared with the authentication data extracted from the shares embedded in the alpha channel plane.Any mismatching indicates the tampering of data.Tampared data is repaired using partial shares in alpha channel plane.The detailed block diagram had been shown in the figure 2.1 and 2.2.

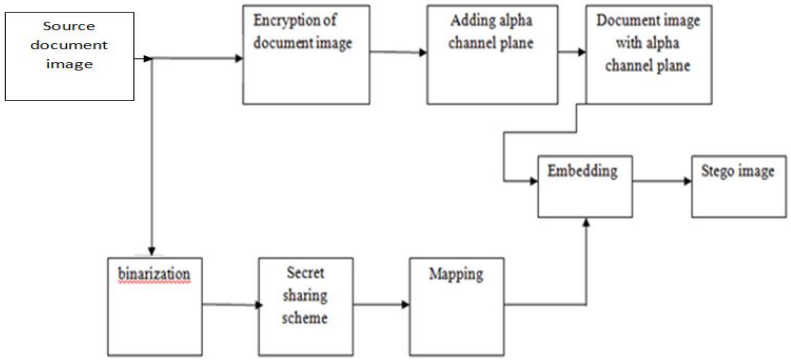

Fig 2.1:Illustration Of Creating Png Image From A Grayscale Document Image And An Alpha Channel

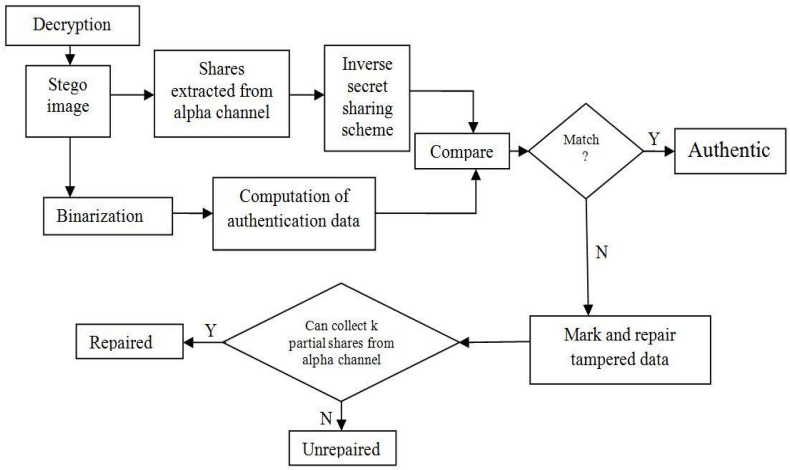

Fig 2.2:Decryption And Authentication Process Including Verification And Self-Reparing Of A Stego –Image In Png Format

III. Overall Algorithm

Algorithm 1: Generation Of Stego Image

Stage I-Creation Of Authentication Signal

Step 1:Binarization of input image using Jarvis half toning.

- Set the threshold value as the average of all pixel values
- Compare the current pixel value with the threshold and print 0 if less than threshold and print 1 if greater than threshold.
- Take error between desired output at that position and printed level.Distribute that error forward to the pixels to be printed.

Step 2:Convert cover image in to PNG format

- Create a new image layer Iα and combine it with I using software package

Step 3:Start looping by taking raster scan of an unprocessed block of order m×n with pixels $p_{1,}p_{2.....}p_n$

Step 4:Generate authentication signals

- Create authentication signal $s=a_1a_{2,}a_1=p_{1XOR}\, p_{2\ XOR}p_3$ and $a_2=p_{4XOR}\, p_{5XOR}p_6$

Stage II:Creation And Embedding Of Shares

Step 1:Creation of data for secret sharing:

- Combine the eight bits of a_1,a_2 and p_1 through p_6 to form an 8-bit string.
- Divide the string in to two 4-bit segments and transform the segments into two decimal values m_1 and m_2 .

Step 2:Partial share generation:

- 6 partial shares is being generated by using the following equation:

  $q_i=F(x_i)=(d+c_ix_i)\text{mod } p$

  Where $d=m_1$ and $c=m_{2,}i=1,2\ldots6,p$ is a primary no.

Step 3:Mapping of partial shares:

- Add 238 to each of q1 through q6 resulting in new values of $q1^{'}$ through $q6^{'}$ respectively .

Step 4:Embedding of two partial shares in the current block:

- Take the block B_α in Iα corresponding to B_b in I_b ,select the first two pixels in B_α in the raster scan order and replace their values by $q_1^{'}$ and $q_2^{'}$ resp..

Step 5:Embedding remaining partial shares at random pixels:

- Use the key to select randomly four pixels in $I_\alpha$and in the raster scan order replace the four pixels values by the remaining four partial squares $q_3^{'}$ through $q_6^{'}$.

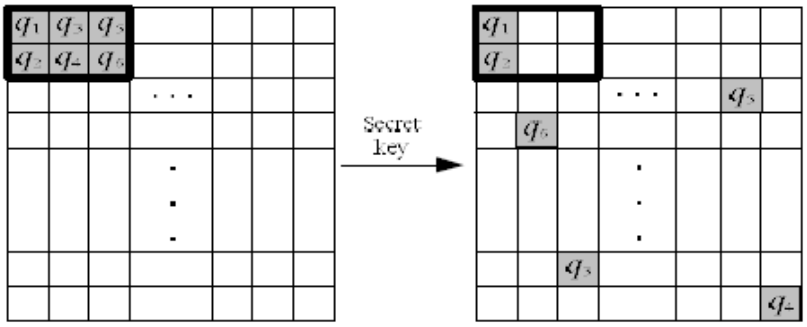

Fig 3.1:illustration of embedding six shares created for a block-two shares embedded at the current block and the other four in four randmoly –selected pixels outside the block,with each selected pixel not being the first two ones in any block.

Algorithm 2:Triple Key Chaotic Encryption Of The Stego Image

Step 1:Forming the binary image matrix

- An image of size N1 x N2 is entered. The pixel values of the image range from 0 to 255. Say, N1 x N2 = N the total number of pixels in the image.
- Each pixel value is converted to its corresponding binary value. k bits are extracted from the binary value of each pixel.
- If the binary representation of the pixel Pi is d1,d2,d3 ••• dN, the result would be an array of size N x k.

Step 2:Computing the Initial Parameter X(i)

- The session key K consisting of 20 hexadecimal characters viz. 0 to 9 and A to F is entered ie is K=k1,k2…k20
- Each hexadecimal character in the session key is converted into its binary equivalent of four bits so that the session key consists of 80 bits
- Two blocks K say k7 ,k8…k12 and k13,k14…k18 24 bit each is being extracted from this and is converted in to corresponding binary value.
- These two values are being xored to obtain the seed value x_{seed}

Step 3:Generating a Chaotic Sequence

- The Chaotic sequence X1,X2X3 ….XN where N is the number of pixels in the image is generated as $x_{i=} \mu x_{seed}(1-x_{seed})$
- Xi is an array of size 1 x N.
- All the values in Xi are converted to their equivalent binary representations. This represents the logistic map B.
- Encrypted data=image data XOR logistic map
- ALGORITHM 3: AUTHENTICATION OF A GIVEN STEGO-IMAGE IN THE PNG FORMAT.

Stage I : Decryption Of The Received Stego Image

- Decryption is same as the encryption process with the knowledge of the session key ,intial parameter and the control parameter.

Stage Ii : Extraction Of The Embedded Two Representative Gray Values.

Step 1:Binarization of the stego-image

- Apply Jarvis half toning technique as explained in algorithm 1 to I to obtain the binary version I_b.

Stage II : Verification Of The Stego-Image

Step 2.:Beginning of looping :

- Scan an unprocessed block B_b' from I_b' with pixel values p_1 through p_6, and find the six pixels' values q1'through q6' of the corresponding block B_α' in the alpha channel plane I_α' of I′.

Step 3. Extraction of the hidden authentication signal:

- Subtract 238 from each of q_1' and q_2' to obtain two partial shares q1 and q2 of Bb′, respectively.
- With the shares (1, q1) and (2, q2) as input, perform lagra two values d and c1 (the secret and the first coefficient value, respectively) as output.
- Transform d and c1 into two 4-bit binary values, concatenate them to form an 8-bit string S, and take the first two bits a1 and a2 of S to compose the hidden authentication signal s = a1a2.

Step 4: Computation of the authentication signal from the current block content

- Compute a two-bit authentication signal $s' = a_1'a_2'$ from the values p1 through p6 of the six pixels of B_b' by $a_1' = p_1 \text{ xor } p_2 \text{ xor } p_3$ and $a_2' = p_4 \text{xor } p_5 \text{xor } p_6$.

Step5.Matching of the hidden and computed authentication signals and marking of tampered blocks

- Match s and s′ by checking if $a_1 = a_1'$ and $a_2 = a_2'$; and if any mismatching occurs, mark B_b, the corresponding block B′ in I′, and all the partial shares embedded in B_b' as tampered .

Step 6. End of looping:

- If there exists any unprocessed block in Ib′, then go to Step 2; otherwise, continue.

STAGE III : SELF-REPAIRING OF THE ORIGINAL IMAGE CONTENT

Step 7. Extraction of the remaining partial shares:

- For each block B_α' in I_α', perform the following steps to extract the remaining four partial shares q_3 through q_6 of the corresponding block B_b' in I_b' from blocks in I_α' other than B_α'.

1. Use the key K to collect the four pixels in I_α' in the same order as they were randomly selected for B_b' in Step 5 of Algorithm 1, and take out the respective data q_3', q_4', q_5', and q_6' embedded in them.
2. Subtract 238 from each of q_3' through q_6' to obtain q_3 through q_6, respectively.

Step 8. Repairing the tampered regions :

- For each block B' in I′ marked as tampered previously, perform the following steps to repair it if possible.

1. From the six partial shares q_1 through q_6 of the block B_b' in I_b' corresponding to B' choose two of them, say q_k and q_1, which are not marked as tampered, if possible.
2. With the shares (k, q_k) and (l, q_1) as input, perform legranges interpolation to extract the values of d and c1 (the secret and the first coefficient value) as output.
3. Transform d and c1 into two 4-bit binary values and concatenate them to form an 8-bit string S′.
4. Take the last six bits b_1', b_2', …, b_6' from S' and check their binary values to repair the corresponding tampered pixel values y_1', y_2', …, y_6' of block B' by the following way:
   if $b_i' = 0$, set $y_i' = g1$; otherwise, set $y_i' = g_2$ where i = 1, 2, …, 6.

Step 9. Take the final *I*′ as the desired self-repaired image *Ir*.

IV. Simulation Outputs

Simulation outputs has been shown in the figures 4.1,4.2,4.3.fig 4.1 indicates formation of stego image and encryption.fig 4.2 indicates the tampering process.fig 4.3 indicate the repairing of the tampered data.

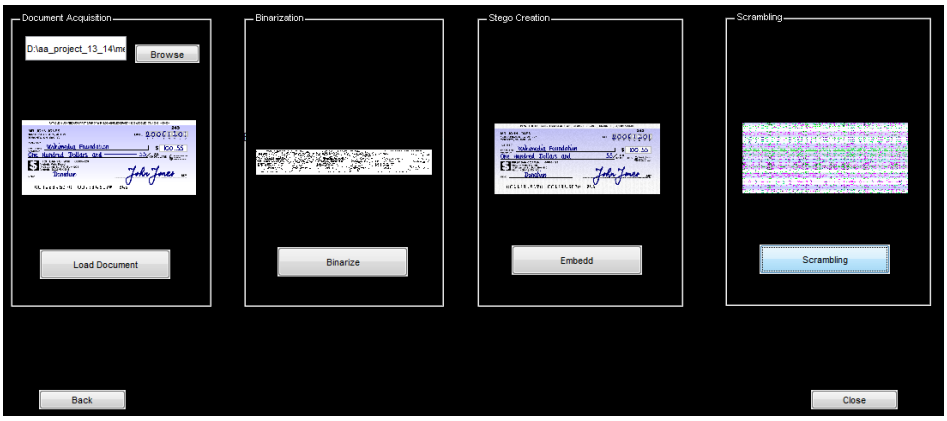

Fig 4.1 Output of Encryption process

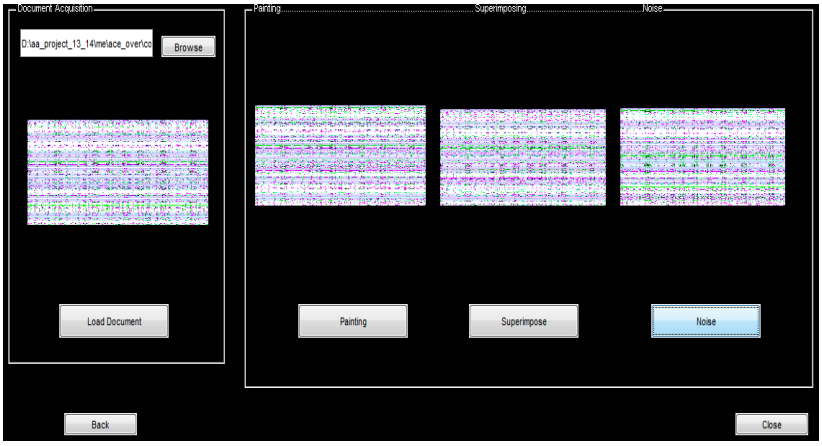

Fig 4.2 Tampering process

Fig 4.3 Repairing process

V. Conclusion

In our work a better security has been implemented for improving that in data transmission by introducing the concept of triple key chaiotic encryption and binarization using Jarvis half toning technique.Document images like cheques while transmitting can be tamoered by the intruder.Here in this paper document is encrypted ,authenticated and trnansmitted.Tampering of data is identified and it is being repaired to regain the original image.

References

[1] Y. Lee, H. Kim, and Y. Park, "A new data hiding scheme for binary image authentication with small image distortion," Information Sci., vol. 179, no. 22, pp. 3866–3884, Nov. 2009.

[2] Y. Lee, J. Hur, H. Kim, Y. Park and H. Yoon, "A new binary image authentication scheme with small distortion and low false negative rates," IEICE Trans. on Communications, vol. E90-B, no. 11, Nov. 2007.

[3] H. Yang and A. C. Kot, "Pattern-based data hiding for binary images authentication by connectivity-preserving," IEEE Trans. on Multimedia, vol. 9, no. 3, pp. 475–486, April 2007.

[4] H. Yang and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier," IEEE Signal Processing Letters, vol. 13, no. 12, pp. 741–744, Dec. 2006.

[5] M. Wu and B. Liu, "Data hiding in binary images for authen- tication and annotation," IEEE Trans.on Multimedia, vol. 6, no. 4, pp. 528–538, Aug. 2004.

[6] W. H. Tsai, "Moment-preserving thresholding: a new approach," Computer Vision, Graphics, and Image Processing, vol. 29, no. 3, pp. 377-393, 1985.

[7] A. Shamir, "How to share a secret," Communication of ACM, vol. 22, pp. 612–613, 1979.