AN ENHANCED AUTHENTICATION TECHNIQUE TO SECURE BIOMETRIC IMAGES

Aruna V, Usha S
Kongu Engineering College, Perundurai
indhuece11@gmail.com, usha@kongu.ac.in

Abstract —

Biometrics images provide the identity of the user based on the physiological or behavioral characteristics of the person. Nowadays, for various purposes, Biometric Images are transmitted over the network. By recent digital technologies, it is possible to attack biometric image. So, to authenticate the biometric images and repaired the tampered images becomes a serious concern. To solve this problem, two enhanced blind authentication techniques are proposed. The first authentication method based on the secret sharing scheme with a data repair capability via the use of the PNG image. In this method, the digital biometric image is combining with the alpha channel to form a PNG image. An authentication signal is transformed into several secret shares by using secret sharing scheme and then embedded into an alpha channel plane of biometric image, which is used for repairing purpose. The second authentication method based on watermarking and bin mapping scheme. In this method, authentication signals are generated by dividing the grayscale range into bins, which provides the double functions of tampering detection and data repairing. Hence, by using these techniques it is possible to authenticate biometric images and also possible to repair if there is any attack in biometric images.

Key words: Biometric Image, Authentication, Repairing, Secret sharing, Bin mapping

I. INTRODUCTION

Biometric Data in form of images are very confidential information of user. If those images are in unauthorized hand then misuse of data may be harmful to authorized user. Biometric images are used in various fields. As in case of Unique ID, each and every citizen of country have their biometric scan images of face, finger,iris and thumb all in original form like JPEG, GIF, etc.

In electronic voting system, the biometric images of voters are collected and stored in database, and at voting time, to allow a citizen to exercise their right to vote by verifying with database if the person satisfies all the requirements needed to vote. Biometric images are also used in various social applications like Indian army. India's national ID method called Aadhaar which is the largest biometric database of the world. Nowadays, many countries are planning to share biometric data with other nations, so it is necessary to give high security to biometric images. Therefore this paper concentrates on providing an algorithm with an enhanced method for authentication of gray scale biometric images with the capability of self-repairing for fixing tampered gray scale image data and parallely answers the problems in the process of image tampering detection by keeping the visual quality of image.

Several methods for binary image authentication have been proposed in the past. C. S. Lu and H. Y. M. Liao [1] proposed a Multipurpose watermarking method for image authentication and protection, M. U. Celik, G. Sharma, E. Saber and A. M. Tekalp [2] develop a secure image authentication method based on Hierarchical watermarking with localization, Z. M. Lu, D. G. Xu and S. H. Sun [3] discussed Multipurpose image watermarking algorithm based on multistage vector quantization for image authentication. Wu and Liu [4] manipulate flippable pixels to create specific relationships to embed data for authentication and annotation of binary images. Yang and Kot [5] discussed a pattern-based data hiding method for binary image authentication in which three transition criteria are used to determine the flippabilities of pixels Kim et al. [6], suggested a method in which a set of pseudo-random pixels in a binary or halftone image are chosen, and authentication codes are computed and inserted into selected random pixels. In Tzeng and Tsai's method [7], authentication codes are generated randomly and embedded into image blocks. Lee et al. [8] proposed a Hamming-code-based data embedding method. Lee et al. [9] improved the method later by using an edge line similarity measure to select flippable pixels. In the method [10], a hierarchical digital watermarking is discussed.

II. EXPERIMENTAL

A. *Authentication based on (k,n) threshold secret sharing algorithm and PNG image*

In (k, n)-threshold secret sharing scheme, a secret message is transformed into n shares and transferred to n participants and when k (k must be less than or equal to n) of the n shares are collected, the secret message can be recovered lossless. Such a secret sharing scheme is useful for reducing the risk of incidental partial data loss.

Algorithm of (k,n) threshold secret sharing scheme,

(1) Choose randomly a prime number p that is larger than secret message d

(2) Select k-1 integer values c1, c2, c3…ck -1 within the range of 0 through p-1.

(3) Select n (number of participant)distinct real values x1, x2, x3,……,xn.

(4) Use the following k-1 degree polynomial to compute n function values F (xi), called partial shares for i=1,2,3,...,n. i.e.,

$$F(x_j) = (d + c_1 x_j + c_2 x_j^2 + \cdots + x_j^{k-1}) \bmod p$$

$$F(x_j) = (d + c_1 x_j + c_2 x_j^2 + \cdots + x_j^{k-1}) \bmod p \quad (1)$$

Algorithm for reverse secret sharing,

(1).From the k shares (x_1, $F(x_1)$), (x_2, $F(x_2)$), (x_k, $F(x_k)$), the generated polynomial,

$$F(x_j) = (d + c_1 x_j + c_2 x_j^2 + \cdots + c_{k-1} x_j^{k-1})$$

(2) Using Lagrange's interpolation to obtain

$$d = (-1)^{k-1}[F(x_1)\frac{x_2 \dots x_k}{(x_1 - x_2)\dots(x_1 - x_k)} + F(x_2)\frac{x_1 x_3 \dots x_k}{(x_2 - x_1)(x_2 - x_3)\dots(x_2 - x_k)} + F(x_1)\frac{x_2 x_3 \dots x_k}{(x_k - x_1)(x_k - x_2)\dots(x_k - x_{k-1})}] mod\ p \quad (3)$$

Compute c1 through ck-1 by

$$F(x) = [F(x_1)\frac{(x-x_2)(x-x_3)\dots(x-x_k)}{(x_1 - x_2)(x_1 - x_3)\dots(x_1 - x_k)} + F(x_2)\frac{(x-x_1)(x-x_3)\dots(x-x_k)}{(x_2 - x_1)(x_2 - x_3)\dots(x_2 - x_k)} + \cdots + F(x_k)\frac{(x-x_1)(x-x_2)\dots(x-x_{k-1})}{(x_k - x_1)(x_k - x_2)\dots(x_k - x_{k-1})}] \bmod p \quad (4)$$

The alpha channel is one of the features of PNG image. It is a color component layer that control and represent the degree of the transparency or opacity of a color. Based on these two methods, authentication of biometric image is proposed. The block diagram of generation of stego image is shown in figure 1

.

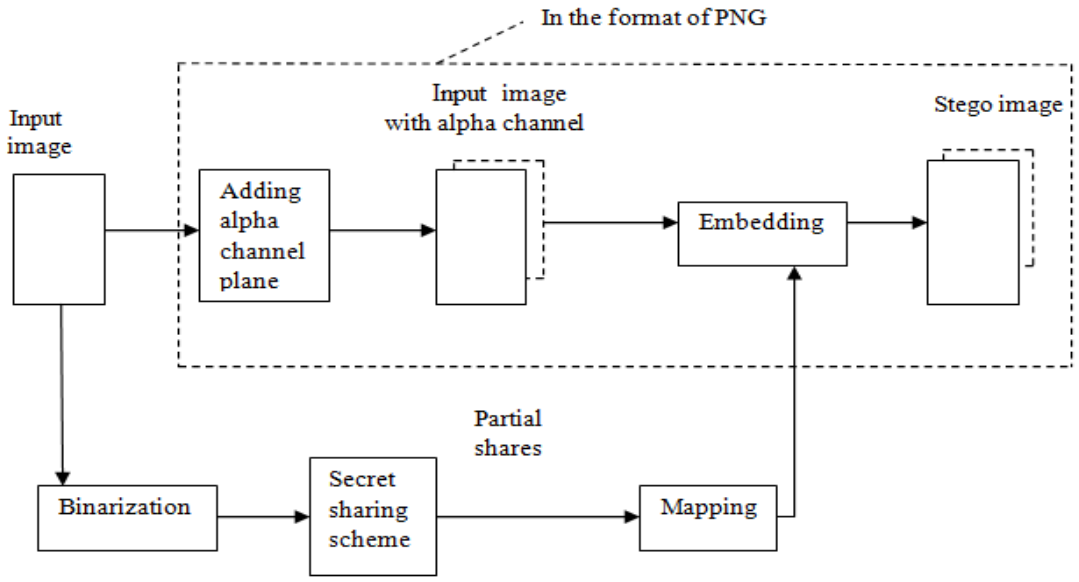

Fig .1. Generation of stego image

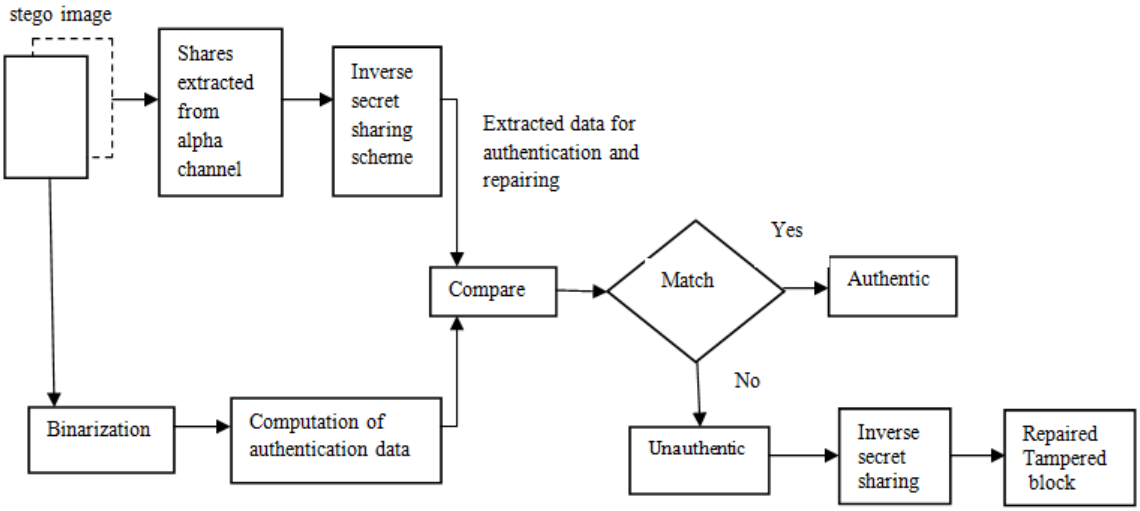

Fig.2. Authentication and repairing attacked stego image

In the generation of stego Image, The biometric input image is binarized and divided into blockwise. And an authentication signal is generated for each block of a biometric image and transformed into partial shares using the Shamir secret sharing scheme. The alpha channel with 100% opacity is created by image processing software and combined to input image which form PNG image. The partial shares are embedded into the alpha channel and considered as stego image.

The stego image is verified in receiver side to check its authenticity by matching the authentication data which is extracted from the alpha channel and from the input image. If both the data are not matched means it is unauthentic block, need to repair that block by reverse secret sharing scheme using the partial shares which are embedded in alpha channel. The block diagram is given in the figure 2.

B. . Authentication based bin mapping scheme

In this method, the grayscale range is divided into bins, a 3-bit bin code is generated as the authentication signal for each pixel in the input cover image. The authentication signals are embedded randomly into the image pixels for the double purposes of tampering localization and data repairing in the image authentication process. This leads to great percentage saving of storage space for embedding signals and recovering purposes, and so results in possibility of authentication in pixel level. Tampered pixel repairing is occurred by retrieving the embedded bin code to obtain a corresponding representative value for use as the new gray value of the tempered pixel.

During the authentication process, for each pixel 'p' in an image, another pixel 'p^1' in an image is selected randomly by the input key 'K'. The five MSBs of pixel 'p' are converted into 3bit bin code by bin mapping scheme which is used as an authentication signal. The authentication signal is embedded into the last three LSBs of the gray value of a corresponding randomly-chosen pixel *'p^1'* which is explained in figure 3

.

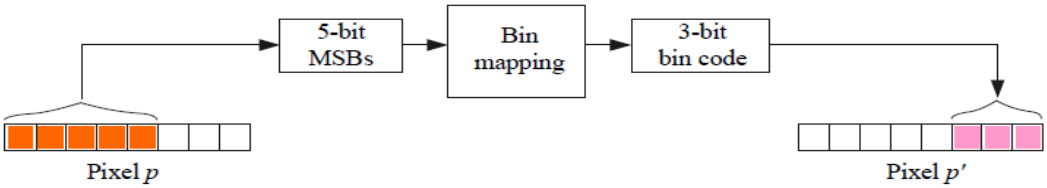

Fig.3 Generation of authentication image

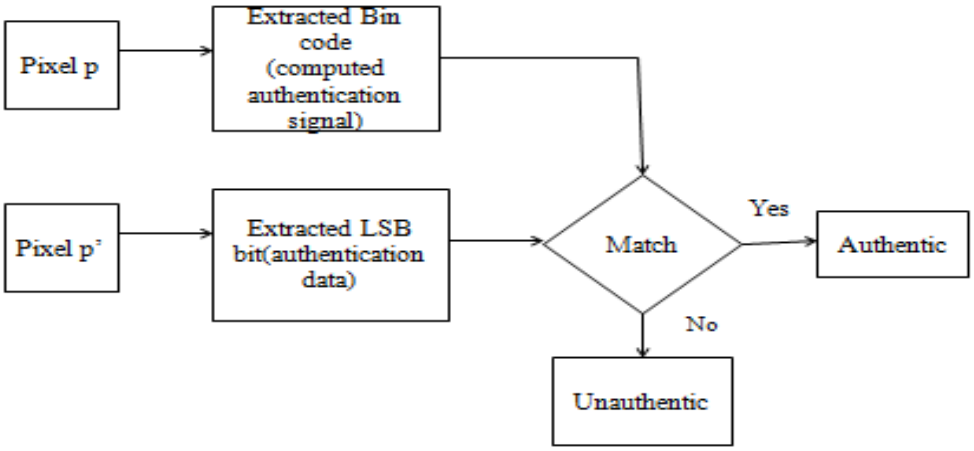

Fig.4. Verification of authentication signal

During verification process, the authentication signal is extracted from the second part of the gray scale value of the randomly selected pixel 'p1' and also the authentication signal is computed from the first part of the gray scale value of the pixel 'p'. The two authentication signals then are compared with each other. If matching occurs, pixel 'p' is regarded as an authentic, otherwise the pixel 'p' is unauthentic. In this case, the second part of the gray value of pixel 'p1' is used as an index to generate the data for repairing the altered gray values of *p* which is shown in figure 4.

During self repairing, the second part LSBs of pixel 'p1' is taken and generated the bin value corresponding to those LSBs according to the table 1 given below. Then by padding three 0's to bin value, 8bit gray scale value is generated which is used to repair the tampered pixel 'p' is explained in figure 5.

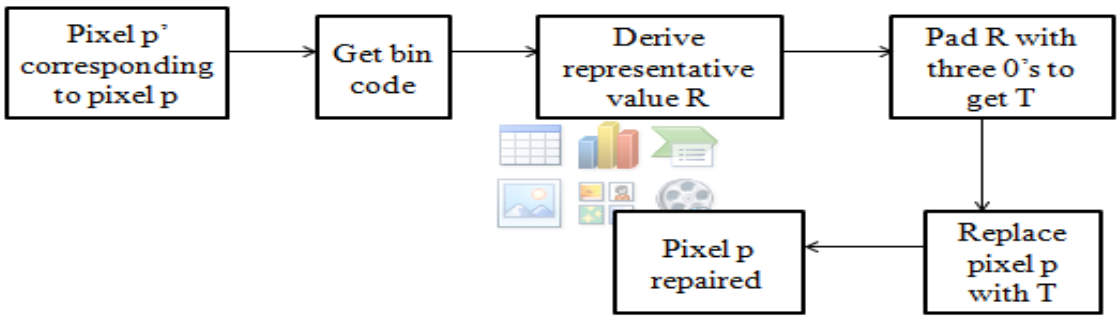

Fig.5. Repairing attacked authentication image

Table1. Bin code and corresponding bin number

Bin	Bin Number	Bin Code	Corresponding Value of Bin
[0,3]	0	000	2
[4,7]	1	001	6
[8,11]	2	010	10
[12,15]	3	011	14
[16,19]	4	100	18
[20,23]	5	101	22
[24,27]	6	110	26
[28,31]	7	111	30

III. RESULTS AND DISCUSSIONS

The objective of the authentication method is to secure the content of the biometric images. So, the input images of the authentication method are various biometric images. Human face, iris, palm, fingerprint are the various biometric images. The Various biometric images are taken as the input and their experimental result is verified for each image by the tool Matlab of 2009(b) version.

Results of secret sharing based authentication method,

In secret sharing based biometric authentication method, the grayscale biometric image is taken as input image of size 300*300. By authentication algorithm, the stego image is generated with partial shares embedding alpha channel which is shown in figure 6.

Fig.6. Generation of stego image

If there is any attack in the received stego image, the attacked tampered block is repaired by using repairing algorithm based on reverse secret sharing scheme which is shown in figure 7.

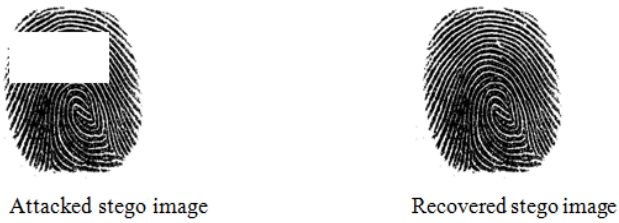

Fig.7. Repairing stego image

The statistics of the performance of the authentication, verification and repairing of the stego image is shown in table 1 results in terms of the five parameters:

1. Tampering Ratio = (the number of tampered blocks)/ (the total number of blocks)
2. Detection Ratio = (the number of detected blocks)/ (the number of tampered blocks)
3. Repair Ratio = (the number of repaired blocks) / (the number of detected blocks)
4. False Acceptance Ratio = (the number of tampered blocks marked as untampered) / (the total number of tampered blocks)
5. False Rejection Ratio = (the number of untampered blocks marked as tampered)/ (the total number of untampered blocks).

Table1. Statistics of performance of authentication method

Image size	No of blocks	Tampering ratio	Detecting ratio	Repairing ratio	False Acceptance ratio	False rejection ratio
300*300	17500	28.1%	100%	100%	0%	0%
418*549	38247	9.5%	100%	100%	0%	0%
400*500	37400	57.9%	100%	100%	0%	0%

In this authentication method, the repairing capability is occur in high efficiency. If the alpha channel is removed from the authentication biometric image during transmission, it is impossible to repair the tampered pixel. This is the main problem occur in this secret sharing based authentication method.

Results of bin mapping scheme based authentication method,

In bin mapping scheme based authentication method, there is no need of extra channel for authentication and repairing purpose. The generation of stego image for the source biometric image is shown in figure 8.

Input image stego image

Fig.8.Generation of stego image

The various attack in the transmitted stego image is repaired by bin code authentication signal which is shown in figure 9. The performance of this bin mapping authentication method is verified by the statistical parameters PSNR,FAR,FRR which is shown in table 2.

Attacked stego Image Repaired stego image

Fig.9. Repairing method.

Table 2. Statistics of performance of bin mapping based authentication method

Imagewith tampering ratio	PSNR value of attacked stego image	False Acceptance ratio	False rejection ratio
0.5%	47.00	0	0
2%	44.63	0	0
5%	39.58	1	4
10%	32.93	12	36
20%	23.19	43	67

In this method, the repairing efficiency is decreased when the tampering ratio is high (i.e) if the attack in the image is greater than 20%, it is not possible to repair the tampered block by this authentication method.

IV. CONCLUSIONS

A new blind image authentication method with a data repair capability for binary-like grayscale biometric images based on secret sharing and bin mapping scheme has been proposed. In secret sharing based authentication method, the authentication and repairing is based on the partial shares of alpha channel. If the alpha channel is removed, then the repairing capability is not possible. This problem is solved by bin mapping authentication method. In bin mapping based authentication method, authentication and self repairing of biometric image is possible based on the bin code authentication signal, but the method is applicable to the biometric images only having low percentage of tampering ratio. Simulation results have been shown to prove the effectiveness of the both authentication method.

REFERENCES

[1] S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," IEEE Trans. on Image Processing, vol. 10, no. 10, pp. 1579–1592,2001

[2] Z. M. Lu, D. G. Xu and S. H. Sun , "Multipurpose image watermarking algorithm based on multistage vector quantization" IEEE Trans. on Image Proc., vol. 14, pp. 822–831,2005.

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

[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. 741–744,2006.

[5] 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. 475–486,2007.

[6] H. Y. Kim and A. Afif , "Secure authentication watermarking for halftone and binary images," Int'l Journal of Imaging Systems and Technology, vol. 14, no. 4, pp. 147–152,2004.

[7] H. Tzeng and W. H. Tsai,. "A new approach to authentication of binary images for multimedia communication with distortion reduction and security enhancement," IEEE Communications Letters, vol. 7, no. 9, pp. 443–445,2012.

[8] 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. 11,2007.

[9] 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. 3866–3884,2009.

[10] P. L. Lin, C. Hsieh and P. Huang, "A hierarchical digital watermarking method for image

[11] tamper detection and recovery," *Patt. Recog.,* no. 38, pp. 2519-2529, 2005.

[12] Y. Park, H. Kang, K, Yamaguchi and K. Kobayashi, "Watermarking for tamper detection

[13] and recovery," *IEICE Electronic Express*, vol. 5, no. 17, pp. 689-696, Sept. 2008.