Secret Sharing Scheme Based Technique for Authentication of Documents Images

Dr. Muna Ghazi
Computer Science Department, University of Technology/ Baghdad
Email: munaalkhiat@yahoo.com
Dr. Hanaa M. A. Salman
Computer Science Department, University of Technology/ Baghdad
Email:salmanhanna2007@yahoo.com

Received on: 18/11/2013 & Accepted on: 3/5/2014

ABSTRACT

Digital document image is a form of persevering important information, and, because of rapid technological development, it is easy to copy, counterfeit this digital document image and claim ownership. Therefore this paper presents a document image authentication scheme based on using secret sharing that can:

1.Authenticate document image.
2.Verify the owner of the document image.
3.Localize the alteration in the document image.
4.Detect the error in the document image, and
5.Correct the error in the document image.

According to comparison of different document image authentication methods, there is no distortion in stego image, the method has capability to locate the tampering, repair capability, reported authentication precision for each (2X3) block, distribution of authenticated image parts in the entire image and manipulating data embedding in LSB(least Signification Bit).

Keywords: Document Image, secret sharing, Authentication,Verification.

تصديق صحة موثوقية النصوص الصورية باستخدام تقنيات مشاركة السرية

الخلاصة

صورة النصوص الرقمية هي شكل من أشكال النسخ الإلكترونية للحفاظ على المعلومات الهامة.لقد اصبحت الصور الرقمية شائعة لذلك فمن السهل نسخ وتزييف مضمون صورة الوثيقة الرقمية وادعاء ملكيتها. هذا البحث يقدم

تقنية لتصديق النصوص الصورية بإستخدام تقنيات المشاركة بالسرية (secret sharingschemes) حيث يمكن ان:

1. المصادقة على صحةالوثيقةِ.
2. يتحقّقْ من مالكَ صورةِ الوثيقةَ.
3. تحديد موضعْ التغيير في صورةِ الوثيقةَ.
4. إكتشافْ الخطأ في صورةِ الوثيقةَ، و
5. تصحيح الخطأ في صورةِ الوثيقةَ.

نتيجة المقارنة مع طرق مختلفة لتصديق صحة النصوص الصوريه تبين، لايوجد تشويه بصورة العلامة المائية، الطريقة لها القابلية على تحديد موقع التزيف، القدرة على التصليح، والمصادقة على كل بلوك بحجم (2×3) ، توزيع اجزاء النصوص الصورية المصدقة في داخل الصورة باستخدام طريقة البت الاقل اهمية.

INTRODUCTION

Digital document image is a form to creating electronic copies to preserve important information and because of rapid development of multimedia and internet applications, hence the digital document image become more and more popular, so it is easy to modify and copy the content of digital document image and claim ownership. Therefore preserving important document images security such as important certificates, signed documents, scanned checks, etc. become necessary issue nowadays. Provide authentication using secret sharing technique is one of the robust solutions to avoid of unauthorized copying or tampering digital document image to ensure the integrity of document image and verify the identity of the owner.

The other necessary issue is the authentication mechanism that will be used to verify the integrity of digital media. The authentication assures that digital media contain no modification, insertion, deletion and the identity of the owner is valid [1]. Generally there are two basic types of authentication: active and passive authentication. Active authentication uses authentication code which is embedded into the digital media. Passive authentication uses the digital media itself without any side information to ensure its integrity [2].

In recent years, many techniques have been proposed to increase the security of the important images, these techniques such as image hiding and watermarking. However, there is a weakness common to all these techniques, is that the secret data are all in single media. Therefore the secret data cannot be revealed completely if the media are lost or corrupted. To overcome this weakness, several secret sharing techniques have been proposed [3].

In 1979, Shamir and Blakely separately have proposed the first concept of (t, n)threshold secret sharing technique, which divides the secret D into n, pieces each piece called share or shadow, which then are distributed among n, participants. In such away only t, or more shares can reconstruct the secret D, where $t \leq n$, but even knowledge $t-1$, or less share, absolutely cannot reveal any information about the secret D[4].

Visual Secret Sharing (VSS) schemes have been proposed over the past decades in many pioneering research. Thien and Lin have adopted Shamir's polynomial secret sharing into secret image sharing in 2002 [3, 5].Wang and Su have made some improvements in Thien and Lin's scheme via decreasing the size of the shared images [5]. Studies in secret image sharing have focused on different topics such as: decrease the size of the share [5,

6], dealing with malicious users' attacks and detecting fake shares [5,7, 8]. The research domain has been extended from gray images to color images [6] and the shares become meaningful instead of using noise [59].Yang [10], Cimato et al [11], and Wang et al [12] have separately proposed new VSS scheme called ProbVSS scheme, which is based on probabilistic concepts for a binary image, this scheme overcomes the problems such as computational complexity and pixel expansion by using Boolean operations.

In 2004, Lin and Tsaihave proposed a new kind of secret image sharing scheme with steganography and authentication, they used parity check to achieve authentication [5,13]. A. M. Namboodiri and A. K. Jain have proposed scheme for authentication of digital documents image that using an on-line signature of the author as watermark to verify the identity of the author and detect changes in the document [14].

In 2007, Yang et al have proposed a new scheme of secret image sharing with steganography and authentication to overcome some of the weaknesses in the Lin-Tsai's scheme by using the concept of hash-based message authentication code instead of parity check to achieve authentication [5, 15].

In 2008, Chang et al have proposed a new scheme of secret image sharing scheme with steganography and authentication to overcome some of the weaknesses in Lin-Tsai's scheme and Yang et al.'s scheme by using the concept of the Chinese Remainder Theorem to achieve authentication [5, 16].

In 2009, Wu et al. have proposed reversible secret image sharing in which the stego images can be recovered to their original state that is not performed in Lin-Tsai's and Yang et al.'s schemes [17].

In 2010, Eslami et al. have proposed a new secret image sharing based on cellular automata instead of Shamir's polynomials that have reduced computational complexity and employed double authentication mechanism to detect tampering, they have also used less number of bits in each pixel of cover images for embedding data so that a better visual quality is guaranteed [18].

In 2011,Wu et al. have proposed another kind of secret image sharing scheme with steganography and authentication, with objective to enhance the quality of the reconstructed secret image by applying pixel adjustment process [19].Eslami and Ahmadabadi have proposed secret image sharing scheme with authentication and dynamic embedding so that the embedding technique uses a non-fixed size blocks, the block size is determined dynamically according to the size of hidden data .Therefore, all the capacity of cover images is used for data hiding [20].

In 2012, Yang et al. have proposed new scheme of (t, n) secret sharing with steganography and authentication by introducing vote-based protocol to provide authentication without needing additional authentication bits, which combine both authentication and secret sharing features into shared bits. The principle of vote-based protocol is that each participant authenticates other shares and votes for shares that he/she trusts so that each share should obtain (t −1) votes from others. The vote-based protocol is based on symmetric bivariate polynomial [21]. Chen and Lin have proposed authentication mechanism for secret sharing using Boolean operation .They compute the authentication of the image using a simple Boolean operation without using complicated process. However, the size of the authentication image is half the size of the secret image, so it cannot authenticate the whole secret image [22].Cimato and Yang have proposed

new scheme for secret image sharing working with grayscale image.They have used two techniques to reduce the size of the cover image ;The first is an error diffusion technique that helps to transform a grayscale image into a binary image, The second is called edge lookup table to improve the quality of the reconstructed grayscale image from binary image, their scheme reduces computational complexity, and authentication ability is much better , also the ratio of cover image size and secret image size is reduced to 2/3 [5]. Lee and Tsai have proposed a method for the authentication of grayscale document images with an additional self-repair capability for fixing tampered image data using secret sharing. They work with binary-like grayscale document image with two major gray values and adding alpha channel plane to the cover image .The authentication process is performed by taking 2*3 block from cover image and Generated two-bit authentication signal [23].

The aim of this paper is to propose authentication technique to the document image, based on using secret sharing schemes that can achieve requirements listed below:

1.Authenticate a document image.
2.Verify the owner of a document image.
3.Localizes the alteration in a document image.
4.Detect the error in a document image, and
5.Correct the error in a document image.

The rest of this paper is, secret sharing is in section 2, the proposed method is in section 3,4 Are experiment results, while section 5. Is conclusions and future works

SECRET SHARING

A secret sharing (SS) can be defined as a technique which distributes shares of a secret to a set of participants whereas specified group of participants can reconstruct the secret by pooling their shares [24].

There are many applications for secret sharing, from these are:
1.Key management and key distribution [4, 24].
2.Multi-party secure protocols [24].
3.Information hiding [5, 13, 15, 16].

There are two main approaches for Secret Sharing, these are [24]:
1.Secret splitting.
2.Secret thresholding.

Secret Splitting

At its simplest level, the secret can be divided into $n$pieces, called shares or shadows, each share by itself means nothing, such that pooling them can be used to reconstruct the secret .Two approaches for secret splitting are [24]:
1.Dual Control by Modular Addition.
2.Unanimous Consent Control by Modular Addition.

Secret Thresholding

At its simplest level, the secret can be divided into $n$pieces, called shares or shadows, each share by itself provides no information, such that any t (threshold) of them can be

used to reconstruct the secret [24, 25]. The threshold secret sharing scheme solves the problem of secret splitting because it requires t of shares to reconstruct the secret not all of the shares so that threshold secret sharing provides secrecy, reliability and flexibility.
Two approaches of secret thresholding and these are [24, 25]:
1- Shamir's (t, n)Threshold secret sharing.
2- Blakley's(t, n)threshold secret sharing.

PROPOSED METHOD

The concept of proposed method is using secret sharing technique as a method for authentication. However, the shares will be used to carry the authentication signals and also help to repair tampered data. The first step will be converting the color cover image to binary image and then dividing it into non overlapping 2×3 blocks. Then, the next step will be the authentication of signal generation, the authentication process is performed for each 2×3 block with pixels $p_1, p_2, p_3, \cdots, p_6$ so it will generate two-bits authentication signals $a_1 = p_1 XOR p_2 XOR p_3$, $a_2 = p_4 XOR p_5 XOR p_6$,thus there will be 8-bits then dividing it into two 4-bits and will convert it into two decimal numbers $dandc$ that represent respectively the secret and coefficient of the Shamir function. The secret contains the 2-bits authentication signals.

The Shamir function performs the Shamir $(2,6)$ threshold scheme which generate six shares whereas the first two shares are embedding in the current block of color cover image which become stego image while the remained four shares are embedding at random pixels chosen by using ID of the person who carries the passport as it will be discussed later in details. After generating six shares for each 2×3 blockthen performing embedding process will be adopted. In order to embedding process will call function (decimal to binary) then perform the embedding in LSB after that will call function (binary to decimal).

The process of chosen random pixels by using the ID to embedding the remains four shares of each block is performed by the following steps: The first step is entering the ID of the person who carries the passport. The second step is taking the ASCII code of the ID and then computing the residue classes to it. The third step is performing the concept of columnar transposition which takes the classes as the key and distributes the columns of the image which do not containthe first two shares of any block then according to columnar transposition will embed the remained shares.

In order to see if there is no distortion in stego image will compare the similarity between cover image and stego image and this is done by using eight types of image quality measures to see the results in different types of measures.
In order to verify the document image (passport), first the cover image will be converted to binary image and then dividing it into non overlapping 2×3 blocks. Then, the next step will compute two-bit authentication signals for each 2×3 block with pixels $p_1, p_2, p_3, \cdots, p_6$ so $a_1' = p_1 XOR p_2 XOR p_3$, $a_2' = p_4 XOR p_5 XOR p_6$then matching the computed authentication signals with extracted hidden authentication signals a_1, a_2 so that if $a_1 = a_1' \; and \; a_2 = a_2'$ for all blocks then the document image (passport) is authentic otherwise the document image (passport) is tampered and also can compute and localize the blocks which are tampered.

Whereas the process of extracting the hidden authentication signals for each block is performed by firstly dividing stego image into non overlapping 2×3 blocks then secondly from each block extracting the two shares from two pixels in first column of the current block; this will be done bycall function (decimal to binary) to extract the share from LSB and after that call function (binary to decimal). Thirdly call function reconstructs for each block to recover the secret. The reconstruct function performs the reconstruction of Shamir $(2,6)$ threshold scheme which take two shares and then recover the secret. Finally the recovered secret will convert to binary bits then extracted the hidden 2-bits authentication signals $a_1 \; and \; a_2$ which used in matching process with computed authentication signals $a_1^{'} \; and \; a_2^{'}$.

The tampered blocks can check its authenticity by extracting the remains four shares which are embedded at random pixels. After extracting the remains shares for each tampered block, matching process will be repeated by taking another two shares until pass matching process (The two shares are reconstructed to recover the secret then extract the hidden authentication signals $a_1 , a_2)$, if any block passes the matching process then the block is repaired otherwise the block is unrepaired. And also it can compute and localize the blocks which are repaired and then compute and localize the blocks which are unrepaired. Therefore if all tampered blocks are repaired then the document image (passport) is authentic otherwise the document image (passport) is unauthentic.

In order to extract the remains shares which are embedded at random pixels, they will enter the ID then follow the same steps as embedding it but using reverse columnar transposition instead of columnar transposition and the extraction process is the same process as extraction the hidden authentication signals from first two shares of each block.

The proposed method is implemented using VB 6, and itconsists of two phases: the first phase is authentication phase which includes sharing and embedding as presented in sub section (4.1), the second phase is verification phase which includes reconstructing and verifying as presented in sub section (4.2).Figure (1) illustrates the framework of the proposed method.

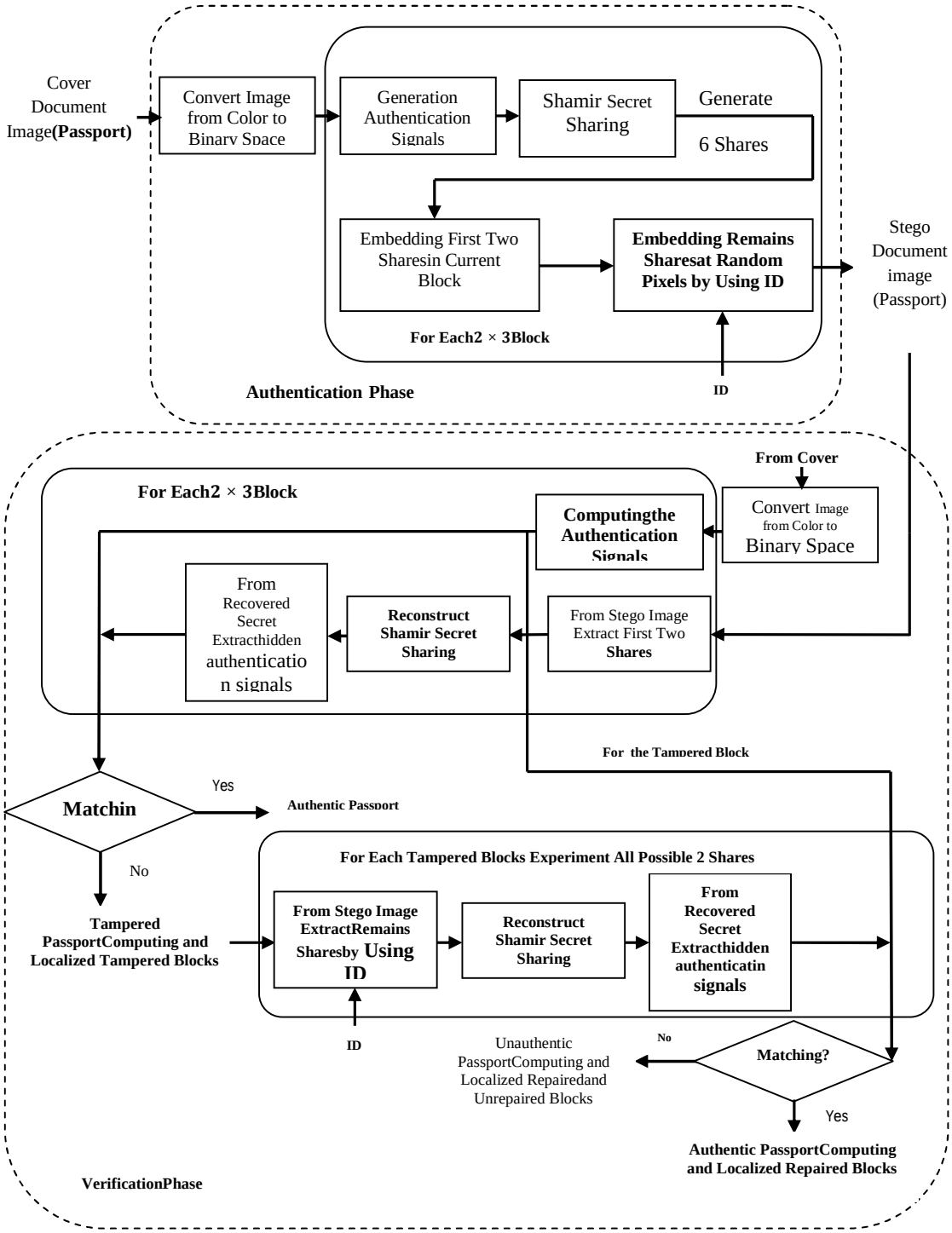


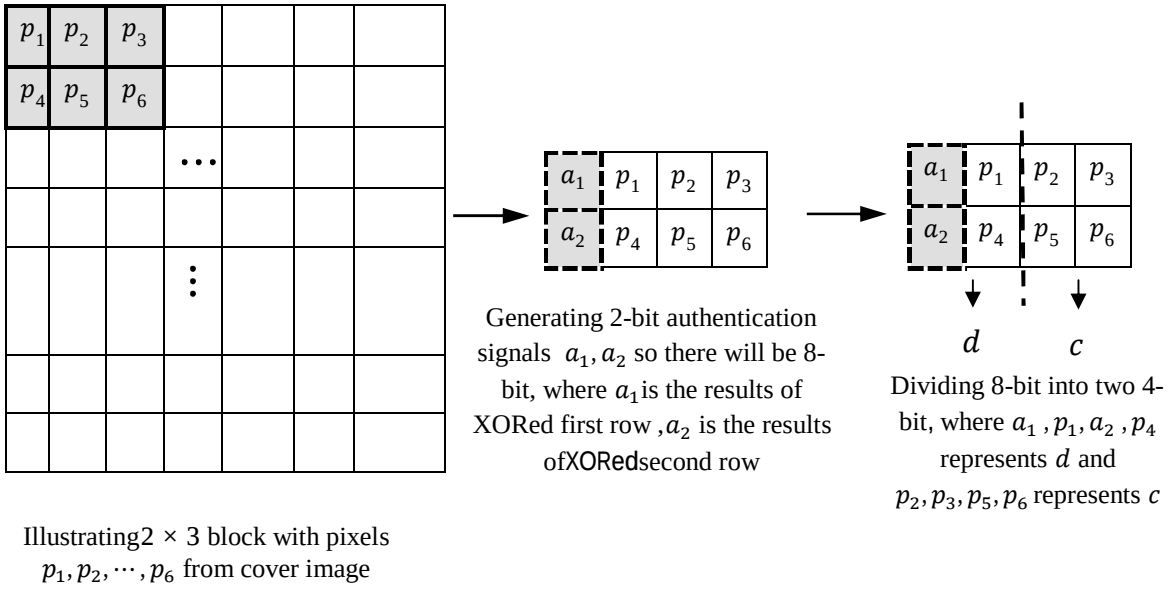
Figure (1):Framework of the Proposed Method

AUTHENTICATION PHASE

The authentication phase is the first phase in proposed method which consists of five steps, including: converting image from color to binary space, generation the authentication signals, Shamir secret sharing, embedding process of first two shares in current block and embedding process of the remains shares at random pixels chosen by using ID. The following is the authentication algorithm.

First step in the authentication phase is converting the color cover image to binary image and then divided it into non overlapping 2×3 blocks.

Second step in authentication phase will be authentication signal generation, the authentication process is performed for each 2×3 block with pixels $p_1, p_2, p_3, \cdots, p_6$ so will generate two-bit authentication signals $a_1 = p_1 \text{XOR} p_2 \text{XOR} p_3$, $a_2 = p_4 \text{XOR} p_5 \text{XOR} p_6$ thus there will be 8-bits $a_1, a_2, p_1, \cdots, p_6$



Illustrating 2×3 block with pixels $p_1, p_2, \cdots, p_6$ from cover image

Generating 2-bit authentication signals a_1, a_2 so there will be 8-bit, where a_1 is the results of XORed first row , a_2 is the results of XORed second row

Dividing 8-bit into two 4-bit, where a_1, p_1, a_2, p_4 represents d and p_2, p_3, p_5, p_6 represents c

Figure (2): Illustration of Generating2-bits Authentication Signals for a Block and Creation the Secret and the Coefficient Values for Secret Sharing

Third step: Shamir (2,6) threshold scheme is used to generate six shares for each block. The d *and* c values of previous step will represent respectively the secret and coefficient values of the Shamir function, and the p prime value of Shamir function will be "17". The 2-bitss authentication signals will be in secret value. Figure (3) illustrates the generation of six shares for a block by using Shamir (2,6) threshold scheme

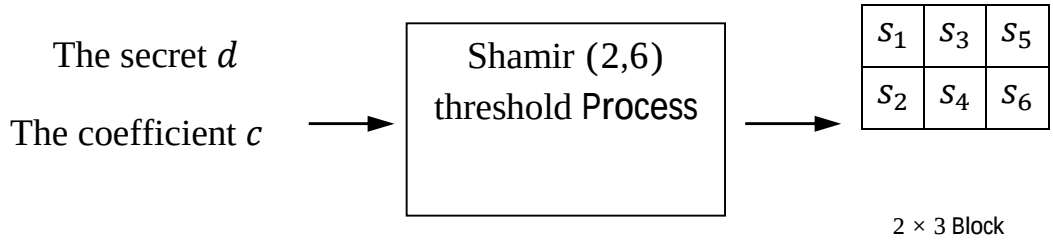


Figure (3):Illustration of Generating Six Shares for a block

Forth step: embedding process of first two shares of each block. The first two shares are embedded in the first column of the current block of color cover image which becomes stego image as illustrated in figure (4), while the remains four shares are embedding at random pixels chosen by using ID**.**

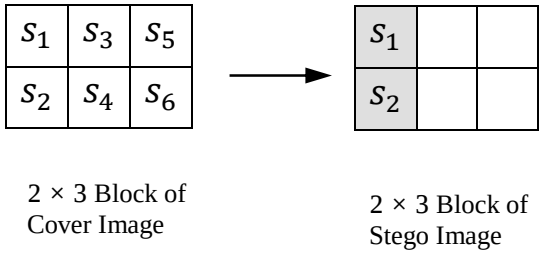


Figure (4):Illustration of Embedding First Two Shares of a Block in the First Column of the Current Block.

Fifth step: embedding process of the remains four shares for each block at random pixels chosen by using ID. The remains shares for each block are embedding at random pixels which don't contain the first two shares of any block, the random pixels are chosen by using the ID of the person who carries the passport, and this is implemented as the following: First entering the ID which represented the e-mail of the person whose carry the passport, getting the ASCII code of the ID, then taking the residue classes of this ASCII code after that using the concept of columnar transposition.

The columnar transposition is implemented by taking the classes as the key (for example if classes are $[2],[1],[3]$ then the key = 213, where the classes are the residue classes of ASCII code of the ID$mod\ 6$) and distributing the columns of the image which do not containthe first two shares of any block (The distribution process as the concept of columnar transposition in distributing alphabets of plaintext on the key whereas in the proposed method distributed numbers represent columns instead of alphabets) to the each sup key(for example if key = 213 then sup keys are 2,1 and 3) then sort the key in ascending order (for example if key = 213 then after sorting the key=123)and take the columns from each sup key to providing new arranging of columns.

Verification Phase

The verification phase is the second phase in proposed method which consists of six steps, including: converting cover image from color to binary space, computation the authentication signals from binary cover image, extraction the hidden authentication signals from stego image, matching the hidden and computed authentication signals to verify of the document image , extraction process of the remained shares by using ID and checking the authenticity of tampered blocks to verify the document image is authentic or unauthentic. The following is the verification algorithm.

First step in the verification phase is converting the color cover image to binary image and then divided it into non overlapping 2×3 blocks.

Second step The second step in verification phase will be computed the authentication signals from binary cover image for each 2×3 block .In this step will be computed the 2-bitss authentication signals $a_1^{'} = p_1 XOR p_2 XOR p_3$, $a_2^{'} = p_4 XOR p_5 XOR p_6$ for each 2×3 block with pixels $p_1, p_2, p_3, \cdots, p_6$,in order to matching the computed authentication signals with extracted hidden authentication signals a_1, a_2 to check the authenticity of the document image.

Third step in verification phase will be extracted the hidden authentication signals from stego image for each 2×3 block from first two shares of each block. In this step for each 2×3 block will extract the hidden 2-bits authentication signals a_1, a_2 from recovered secret of two shares from two pixels in first column of the current block.

Forth step in verification phase will be matched the hidden and computed authentication signals for each 2×3 block to verify the document image is authentic or tampered.

In this step for each 2×3 block will be matched 2-bits extracted hidden authentication signals a_1, a_2 with 2-bits computed authentication signals $a_1^{'}, a_2^{'}$ to verify of the document image (passport) is authentic or tampered, so that if $a_1 = a_1^{'} \; and \; a_2 = a_2^{'}$ for all blocks then the document image (passport) is authentic, otherwiseif any mismatch occurs then the document image (passport) is tampered so that will compute and localize the blocks which are tampered.

Fifth step in verification phase will be extracted process of the remains shares by using ID. In order to check the authenticity of tampered blocks will extract the remained shares for each 2×3 block by using ID.

The process of extracting the remained shares by using ID implemented as the following: Firstly, entering the ID which represents the e-mail of the person who carries the passport same as the ID in authentication phase, getting the ASCII code of the ID, then taking the residue classes of this ASCII code after that using the concept of reverse columnar transposition.

Sixth step in verification phase will check the authenticity of tampered blocks to verify the document image is authentic or unauthentic. The tampered blocks will check its authenticity (if the block is affected by acceptable manipulations) by entering the ID of the person who carries the passport to get the remains four shares for each tampered block as illustrated in fifth step of verification phase.

After that the secret will be recovered for each tampered block by reconstruction of Shamir $(2,6)$ threshold scheme which takes any two shares from the extraction of the remained four shares then getting the hidden 2-bitsauthentication signals a_1, a_2 .

Repeat matching process for each tampered block if any block passes the matching process then the block is repaired otherwise the block is unrepaired. Also it will compute and localize the blocks which are repaired, and then compute and localize the blocks which are unrepaired. Therefore if all tampered blocks are repaired then the document image (passport) is authentic otherwise the document image (passport) is unauthentic.

EXPERIMENTS RESULTS

This section will present experiments results for image quality measures for comparison process between cover and stego image. The eight types of image quality measures (Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR), Peak signal-to-noise ratio (PSNR) , Normalized Cross-Correlation (NK), Average Difference (AD), Structural Content (SC), Maximum Difference (MD) , Laplacian Mean Square Error (LMSE), Normalized Absolute Error (NAE))have been tested to find out the similarity between the cover and stego image of the proposed method. Table (1) shows the results of quality measures of passport images.

Table (1): The quality measures results of the passport images test

Measures / Test Images	MSE	PSNR	NK	AD	SC	MD	LMSE	NAE
Passport image 1	1.818	45.533	0.998	0.238	1.002	2.333	4.053	5.561
Passport image 2	1.926	45.283	0.998	0.27	1.002	2.333	3.754	4.899
Passport image 3	1.878	45.393	0.998	0.222	1.002	2.333	2.418	4.782
Passport image 4	1.892	45.359	0.998	0.246	1.002	2.333	2.159	4.853
Passport image 5	1.954	45.219	0.998	0.354	1.003	2.333	2.72	5.975
Passport image 6	1.956	45.215	0.998	0.286	1.002	2.333	3.474	4.931
Passport image 7	2.013	45.092	0.997	0.434	1.004	2.333	7.699	6.42
Passport image 8	2.042	45.029	0.997	0.467	1.004	2.333	7.395	7.552
Passport image 9	1.292	45.277	0.998	0.288	1.002	2.333	2.65	5.835
Passport image 10	1.864	45.425	0.998	0.27	1.003	2.333	4.247	6.421

According to table (1) there is no distortion in the stego image when applying the proposed authentication method to the test images.
Table (2) showscomparison of performances with other methods.

Table (2): Comparison of different document image authentication methods

	Distortion in Stego-image	Tampering Localization Capability	Repair Capability	Reported Authentication precision	Distribution of authenticated image parts	Manipulation of data embedding
Wu & Liu [26]	Yes	No	No	Macro-block	Non-blank part	Pixel flippability
Yang & Kot [27]	Yes	Yes	No	33×33 block	Non-blank part	Pixel flippability
Yang& Kot [28]	Yes	No	No	Macro-block	Non-blank part	Pixel flippability
Tzeng& Tsai [29]	Yes	Yes	No	64×64 block	Entire image	Pixel replacement
Lee& Tsai[23]	No	Yes	Yes	2×3 block	Entire image	Alpha channel Pixel replacement
kavitha&Shanavas [30]	No	Yes	Yes	2×3 block	Only at strong points in the image	Adaptive mod 4 Embedding.
The proposed method	No	Yes	Yes	2×3 block	Entire image	LSB

CONCLUSIONS AND FUTURE WORKS

The proposed method has reached to the following conclusions:-

1- This method uses Shamir(t, n)secret sharing for authentication and error correction.

2- Enhancing data security by using secret sharing.

3-This is the first method that uses colored representation of document image as cover, and its binary representation as a hidden message, with respect to the authentication of the document images.

4-The first way is to provide dual use of the (ID), where it is used as a random generator to yield a random hash keys that are used for the embedding process and also used as a means to verify the identity of the owner.

5- The use of block size measuring (2×3) is very convenient because a larger block size will reduce the integrity of authentication while a smaller block size means the block can be used to embed shares less than six and that will reduce the repair capability.

6- The proposed method has good performance measures.

The possible Future works take several directions including:

1- Applying of the proposed method for image authentication.

2- Using the signature of the person as the ID to verify the owner instead of the e-mail of the person as the ID. Block based owner validation may also be applied.

3- Using the technique of secret sharing to provide RNG (Random Number Generator), by taking the ID as the secret value then generating several shares as needed then these shares can be used as random locations.

4- Embedding shares in frequency domain that provides high security and also can improve data repairing.

REFERENCES

[1] W. Stallings, "Cryptography and Network Security: Principles and Practice", Fifth Edition, Prentice Hall, 2011.

[2] A. D'Angelo, G.Cancelli and M. Barni ,"Watermark-Based Authentication", Springer-Verlag Berlin Heidelberg, Vol. 282, Pp.365 -402, 2010.

[3] C.C. Thien and J.C. Lin, "Secret Image Sharing", Elsevier, Computers and Graphics, Vol. 26, No. 5, pp. 765-770, 2002.

[4] A. Shamir, "How to Share a Secret", Communications of the ACM, Vol. 22, No. 11, pp. 612–613, 1979.

[5] S.Cimato and C.-N. Yang, "Visual Cryptography and Secret Image Sharing", CRC Press/ Taylor & Francis Group, 2012.

[6] C.-C. Chang, C.-C. Lin, C.-H. Lin and Y.-H. Chen, "A Novel Secret Image Sharing Scheme in Color Images Using Small Shadow Images", Information Sciences, Vol. 178, No. 11, pp. 2433-2447, 2008.

[7] G. Horng, T. Chen, and D. Tasi," Cheating in Visual Cryptography", Designs, Codes and Cryptography, Vol. 38, pp. 219-236, 2006.

[8] P.-Y. Lin," Media Sharing Scheme with Cheater Identification and Content Reconstruction", Journal of Electronic Science and Technology, Vol. 9, No. 4, December 2011.

[9] C.C. Thien and J.C. Lin, "An Image-Sharing Scheme with User-Friendly Shadow Images", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 13, No. 12, pp. 1161-1169,2003.

[10] N. Yang, "New Visual Secret Sharing Schemes Using Probabilistic Schemes", Pattern Recognition Letters, Vol. 25, No. 4, pp.481-494,2004.

[11] S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic Visual Cryptography Schemes", the Computer Journal, Vol. 49, No. 1, pp. 97-107, 2006.

[12] A. Wang, L. Zhang, N. Ma, and X. Li, "Two Secret Sharing Schemes Based on Boolean Operations", Pattern Recognition, Vol. 40,pp. 2776 -2785, 2007.

[13] C.C. Lin and W.H. Tsai, "Secret Image Sharing with Steganography And Authentication", Elsevier, Journal of Systems and Software, Vol.73, No. 3, pp. 405-414, 2004.

[14] A. M. Namboodiri and A. K. Jain," Multimedia Document Authentication using On-line Signatures as Watermarks",Proceedings of SPIE, Vol. 5306, pp. 653-662, 2004.

[15] C.-N. Yang, T.S. Chen, K.H. Yu, and C.C. Wang," Improvements of Image Sharing with Steganography and Authentication", Journal of Systems and Software, Vol. 80, No. 7, pp. 1070-1076, 2007.

[16] C.C. Chang, Y.P. Hsieh, and C.H. Lin, "Sharing Secrets in Stego- Images with Authentication", Elsevier, Pattern Recognition, Vol. 41,No. 10, pp. 3130-3137, 2008.

[17] C. C. Wu, S. J. Kao,W. C. Kuo and M. S. Hwang," Reversible Secret Image Sharing Based on Shamir's Scheme", IEEE Intelligent Information Hiding and Multimedia Signal Processing, pp. 1014 – 1017,12-14 Sept. 2009.

[18] Z. Eslami, S.H. Razzaghi and J.Z. Ahmadabadi," Secret Image Sharing Based on Cellular Automata and Steganography", Elsevier, Pattern Recognition, Vol. 43, pp. 397 – 404, 2010.

[19] C. C. Wu, S. J. Kao and M. S. Hwang,"A High Quality Image Sharing With Steganography and Adaptive Authentication Scheme", Elsevier, Journal of Systems and Software,Vol. 84, Issue12, Pages 2196–2207, December 2011.
[20] Z. Eslami and J.Z. Ahmadabadi," Secret Image Sharing with Authentication-Chaining and Dynamic Embedding",Elsevier,Journal of Systems and Software,Vol.84, Issue 5, Pages 803–809, May 2011.
[21] C.-N. Yang, J.-F.Ouyang and L.Harn," Steganography and Authentication in Image Sharing without Parity Bits", Elsevier, Optics Communications, Vol. 285, Issue 7, pp. 1725–1735, 2012.
[22] Y.-H. Chen and P.-Y. Lin," Authentication Mechanism for Secret Sharing Using Boolean Operation", Journal of Electronic Science and Technology, Vol. 10, No. 3, Septemper 2012.
[23] C.-W. Leeand W.-H. Tsai, "A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use Of the PNG Image With a Data Repair Capability", IEEE Transactions on Image Processing, Vol. 21, No. 1, January 2012.
[24] J. Leiwo, "Secret Sharing", Nanyang Technological University,2004,URL:http://www.tml.hut.fi/Studies/T110.447/2004/secret sharing.pdf
[25] I. Minevskiy," Construction of a Secret Sharing Scheme with Multiple Extra Functionalities ", the University of British Columbia, 2004.
[26] M. Wu and B. Liu, "Data Hiding in Binary Images for Authentication and Annotation", IEEE Transactions on Multimedia, Vol. 6, No. 4, pp. 528-538, Aug. 2004.
[27] H. Yang and A. C. Kot, "Binary Image Authentication with Tampering Localization by Embedding Cryptographic Signature and Block Identifier" , IEEE Signal Process, vol. 13, No. 12, pp. 741–744, Dec.2006.
[28] H. Yang and A. C. Kot, "Pattern-Based Data Hiding for Binary Images Authentication by Connectivity-Preserving", IEEE Transactions on Multimedia, Vol. 9, No. 3, pp. 475–486, Apr. 2007.
[29] C. 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, Sep. 2003.
[30] S. Kavitha and Shanavas K A, "Secure Image Authentication of a Grayscale Document using Secret Sharing Method and Chaotic Logistic Map with Data Repair Capability",International Journal of Innovative Technology and Exploring Engineering Vol. 2,No. 6,May 2013.