International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 10, Issue 1, January- February 2019, pp. 11-19, Article ID: IJARET_10_01_002
Available online at http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=10&IType=01
ISSN Print: 0976-6480 and ISSN Online: 0976-6499

A REVIEW PAPER ON IMAGE AUTHENTICATION SCHEME

Anushri Shinde, Prital Salunkhe, Prajakta Mane
BE Student
Department of Electronics & Telecommunication Engineering
AITRC Vita, India.

Arjun Nichal
Assistant Professor
Department of Electronics & Telecommunication Engineering
AITRC Vita, India.

ABSTRACT

Image authentication is one of the methods which can detect the any tampering data. The original grayscale document image is converted into stego image by adding the alpha channel plane. The stego image is in the Portable Network Graphics (PNG) format. This stego image is transmitted over the network. The authentication process is applied on the stego image on the receiver side. In the authentication process the data extracted from this stego image is compared with the data computed from the binary version of the stego image. If the data is matched the image is considered to be authentic. Else the tampered blocks are marked and the image is self-repaired using inverse secret sharing scheme.but in other methods they cannot resist the self-substitution attack, the same-position-substitution attack, or the cut- off attack. Furthermore, those attacks can be completed by the popular image editing software Adobe Photoshop. We proposed security enhanced authentication scheme. Our proposed scheme is capable of repairing the content of the given stego-image if attacked by the methods mentioned above.

Keywords: Data hiding, watermarking, authentication, tampering, data repair, grayscale image

Cite this Article: Anushri Shinde, Prital Salunkhe, Prajakta Mane and Arjun Nichal, A Review Paper on Image Authentication Scheme International Journal of Advanced Research in Engineering and Technology, 10(1), 2019, pp 11-19.
http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=10&IType=1

1. INTRODUCTION

Authentication is the process or action of verifying the identity of user or process. Image authentication technique have a recently gained great attention due to its importance for a large number of multimedia application. With the fast development of information technology, the digital image has become an important way of preserving and communicating important

information; however, the wide application of image editing software makes it easy to modify the contents of digital images without visual perception. Therefore, how to ensure the credibility of image content has become a challenge. Image authentication technology is an efficient method of overcoming this challenge. Among all kinds of the images, the document images need more protection. The reason is that a document image consists of text, tables, line art, etc., and a little change in it can cause a large amount of meaning to be changed. Therefore, authentication of a document image is more meaningful for practical application. Digital image can be used to preserve important information such as important certificates, signed documents, scanned checks, circuit diagrams, art drawings, design drafts, last will and testaments, and so on. Image transmission is a major activity in today's communication. Digital images are now widely distributed via the inter-net and various public channels. With the advance of digital technologies; it is now easy to modify digital images without causing noticeable changes, resulting possibly in tampering of transmitted images. It is desirable to design effective method for image authentication, aiming to check the fidelity and integrity of received images. Authentication without any perceptible distortion as well as ability to repair tampered image parts. In this method the original image is binary like grayscale image. This image is transformed into a stego image which is in the PNG format. PNG is an extension to the stego image. This image is then sent to the receiver. The stego image is then verified by the proposed authentication method. If the image has not undergone any attack it is verified. Otherwise, the tampered blocks are identified and the image is repaired using reverse Shamir secret sharing scheme. The Lee and Tsai's mehods claim that their method has merits e.g., pixel-level repair capability, higher possibility of attacked content surviving, a new type of data hiding, no distortion for a given image, and enhancing data security by secret sharing. Most of these claims are correct; however, the method has some security flaws. The authentication process can be completed in an independent block without a secret value. Therefore, if we replace some blocks of the stego-image from other position of itself (known as a self-substitution attack) or the same position of another stego-image (known as a same position-substitution attack), or cut off some rows (columns) (known as cut-off attack) without keeping the size of the original stego-image invariant. These attack operations are very common for images but cause a greater amount of meaning to be changed for comparing with the original document image. It is easy to resist the self-substitution attack and the same-position substitution attack; however, it is difficult to resist the cut-off attack. Our scheme can detect and repair the self-substitution attack and same-position-substitution attack. For every pixel of the binary version image, we randomized it by using exclusive-or method with a random binary sequence generated by the secret value and the given image's identity. Therefore, when we replace some blocks of the stego-image from other position of itself or from the same position of another stego-image of the same size, our scheme can detect the substitution attack because the authentication signals of different blocks are relevant by using exclusive-or method with a different random binary sequence. Our scheme can repair the substitutional blocks.

2. METHODOLOGY

The proposed method which aims to authenticate the gray scale image and after detection of tampering in original image, the method is also able to repair the tampered areas of the image. The proposed method is based on the secret sharing scheme using concept of random sequences. Conventionally, the concepts of secret sharing and data hiding for image authentication are two irrelevant issues in the domain of information security. In the proposed method, we combine them together to develop a new image authentication technique.

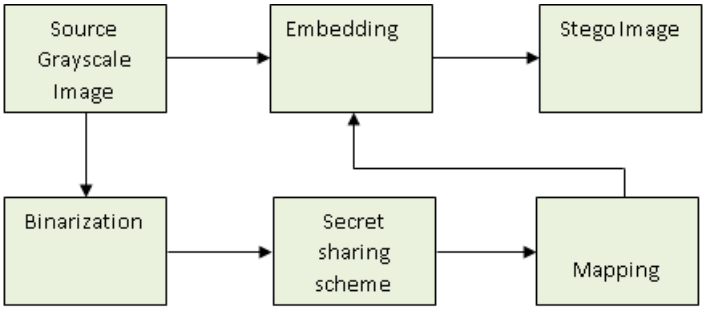

Figure 1 Creation of Stego Image from Grayscale Image

In case of 1st image, the source image is gray scale document image. The intermediate step of binarization of image. The image is then given as input to the algorithm for generation of Stego-image which is very similar to grayscale image, but it is authentic image, as the data for authentication and Self repairing is embedded into it. Now tampering is done as the title of the document is altered with name Test image. Then after applying the authentication algorithm to it, it will successfully detect the tampered blocks and marked them as white, followed by the data repair result. The results are taken from the Matlab Output Window for better understanding. In that a method of document image authentication with an additional self-repair capability to fix data of tampered image. The input cover image is presumed to be a like a binary grayscale image with two major gray values like the one shown in Fig. 1. After the proposed method is applied, the cover image is altered into a stego-image with the Portable Network Graphics format with an additional alpha channel for network transmission or archiving in the databases. The stegoimage, when either received or retrieved, may be verified by the proposed method for its authenticity. Detection of integrity modifications of the stego-image can be done by the method at the block level and repaired at the pixel level. In case of removal of alpha channel from the stego-image entirely, the complete resulting image is considered as inauthentic, which means that the image fails the fidelity check. The proposed method is based on the (k, n)-scheme of threshold secret sharing proposed by Shamir in which transformation of a secret message is done into n shares in order to keep by n participants; and when k of the n shares are collected, not necessarily all of them, we can have a lossless recovery of the secret message. Such a scheme of secret sharing is beneficial to reduce the risk of incidental partial data loss. Usually, the concepts of “secret sharing” and “data hiding for image authentication” are two unrelated issues in the area of information security. But in the proposed method, we have combined them together for developing a novel image authentication technique. The secret sharing scheme is used in the developed technique not just to transmit authentication signals along with image content data, but also to assist towards repairing of the tampered data through the use of shares. A major topic of discussion in the self-repairing of tampered data at attacked image parts is that, after the original cover image data is embedded into the image itself to use in data repairing later on, the cover image is itself destroyed in the first place and the original data is now no longer available for the purpose of data repairing, which results in a contradiction. A solution to this difficulty is to embed the original image data somewhere else without varying the cover image itself. The technique proposed in this paper to implement this solution is to utilize the extra alpha channel in a PNG image so as to embed the original image data. However, the use of alpha channel of the PNG image is done to create a desired degree of transparency for the image. Moreover, data embedding into the alpha channel will create random transparency in the resulting PNG image, which will produce an unwanted opaque effect. In this paper, is to map the resulting alpha channel values into a small range near their extreme value of 255, resulting in an almost undetectable transparency effect on the plane of alpha channel. There is another difficulty faced during the self-repairing of the original image data, that the data to be embedded in the carrier are often large in size. This is not a problem for

our case where with the alpha channel as the carrier, the cover image that is dealt with is basically binary-like, and hence, we may just embed into the carrier a binary version of the cover image, which includes much less data. Additionally, through a cautious design of authentication signals, an appropriate selection of the basic authentication unit (i.e., the unit of 2 x 3 image block) and a good parameter adjustment in the Shamir scheme, we can reduce the data volume of the generated shares commendably so that more shares can be embedded into the alpha channel plane. It is noted that, by the proposed method, the larger the number of shares is, the higher will be the resulting data repair capability.

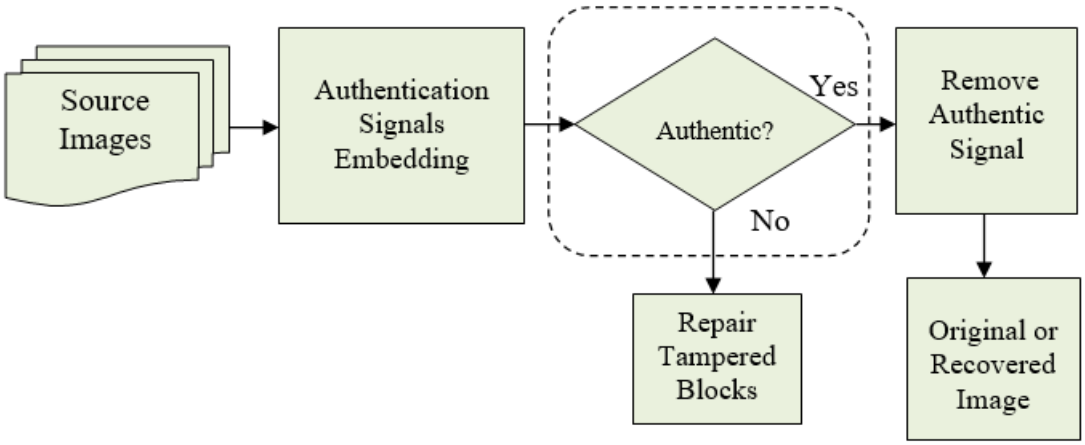

Figure.2. Framework of proposed document image Authentication method

We allocate the multiple shares in a random manner into the alpha channel to allow the share data to have great likelihoods of surviving attacks and to thus stimulate the data repair capability. To the best of our knowledge, this can be considered to be the first secret-sharing-based authentication method for binary-like grayscale document images. It is also the first authentication method for such document images through the use of the PNG image. It is also worth noting that this method is not a secret-sharing technique but a method of document image authentication. And in that method resist the self-substitution attack, the same-position-substitution attack, or the cut- off attack.

3. LITERATURE REVIEW

In 2016, Feng Wang & Won-Li-Lyu, Jung Shyang-Pan [1] proposed a Robust image authentication scheme with self-repair capability for gray scale source document images via PNG format. In that he proposed a new authentication method which is based on the Lee & Tsai method but in that method, he can resist the self-substitution attack, the same position substitution attack or the cut off attack. those attacks can be completed by the popular image editing software Adobe Photoshop. He proposed scheme uses three random binary sequences to randomize the binary version of a given gray scale document image, and thus overcomes the security flaws mentioned above. The authors proposed scheme is capable of repairing the content of the given stego-image if attacked by the methods mentioned above & he proposed scheme retains all of the strengths of Lee and Tsai's scheme. The authors improve the opacity of the alpha channel of stego-image by using Wang and Su's extended secret sharing, and enhance the data security by using Hash functions.

In 2015, Patel Roshani, Prof Aslam Durvesh,etl [2] proposed Lossless Method for Data Hiding In Encrypted Image. In that he proposed the concept presents an idea to embed data in an encrypted image by using an irreversible approach of data hiding or data hiding, aimed at secretly embedding a message into the data. Massage communication over internet facing

problems like data security, copyright control, data size capacity, authentication etc. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. The aim of this dissertation is to create a secure data hiding technology. The data hiding and image encryption are done by using two different keys. That is encryption key and the data hiding key. So, the receiver who has the data hiding key can retrieve the data embedded.

In 2014, K.V.Arya & Akanksha Bandil [3] proposed An Improved Image Authentication Technique using RandomSequence based Secret-Sharing Scheme. In that he proposed the method to repair the tampered areas of the image. There are two methods are used for image authentication. First is having the digital signature or to embed a secret code in the image. A security and protection of digital documents such as important certificates, scanned check, signed document are so imporatant.so the authenticity is very important for now a days. An authentication signals is generated together with binarized block which is transformed into several shares using secret sharing scheme. In this authentication of gray scale image and after detection of tampering in original image. This scheme is used for security protection and data repair capabilities.

In 2012, Che-Wei-Lee & Wen Hsiang Tsai [4] proposed A Secret-Sharing-Based Method for Authentication of Gray scale Document Images via the Use of the PNG Image with a Data Repair Capability. In that he proposed an authentication signal is generated for each block of a gray scale document image, which, together with the binarized block content, is transformed into several shares using the Shamir secret sharing scheme. The involved parameters are carefully chosen so that as many shares as possible are generated and embedded into an alpha channel plane. The alpha channel plane is then combined with the original gray scale image to form a PNG image. Measures for protecting the security of the data hidden in the alpha channel are also proposed. Good experimental results prove the effectiveness of the proposed method for real applications.

In 2010, Meng Guo& Hangbin Zhang [5] proposed High Capacity Data Hiding for Binary Image Authentication. In that he proposed data hiding scheme with high capacity for binary images, including document images, halftone images, scanned figures, text and signatures. In that, the embedding efficiency and the placement of embedding changes are considered simultaneously. Given a M×N image block, the upper bound of the number of bits that can be embedded of the scheme is nlog2((M×N)/n + 1) by changing at most n pixels. this method can embed more data, meanwhile maintain a better quality, and have wider applications than existing schemes.

In 2009, Nabin Ghosh all, J. K. Mandal, etl. [6] Proposed Image Authentication by Hiding Large Volume of Data and Secure Message Transmission Technique using Mask. In that he proposed. An image authentication and secures message transmission technique by embedding message/image into color images. Authentication is done by embedding message/ image by choosing image blocks of size 3 x 3 called mask from the source image in row major order. The dimension of authenticating image followed by MD-5 key and then the content of authenticating message/image are also embedded. This is followed by an XOR operation of the embedded image with another self-generated MD-5 key obtained from the source image applying the reverse algorithm. The result has been tested with the aid of Histogram analysis, noise analysis and standard deviation computation of the source image with the embedded image and has been compared with popular existing steganographic algorithms like S-Tools where the proposed IAHLVDDSMTTM is capable to hide large volume of data than S-Tools and shows better performance.

In 2008, Chin-Chen Chang,Wei-Liang Tai&Kuo-Nan Chen [7] proposed a Lossless Data Hiding Based on Histogram Modification for Image Authentication. In that he proposed

Lossless data hiding enables the embedding of messages in a host image without any loss of content. In this paper, he presents a lossless data hiding technique based on histogram modification for image authentication that is lossless in the sense that if the marked image is deemed authentic, the embedding distortion can be completely removed from the marked image after the embedded message has been extracted. This technique uses characteristics of the pixel difference to embed more data than other histogram based lossless data hiding algorithms. He also presents a histogram shifting technique to prevent overflow and underflow problems. Performance comparisons with other existing lossless data hiding schemes are provided to demonstrate the superiority of the proposed scheme.

In 2008, Ankur Dauneria, Kumari Indu [8] proposed Encryption Based Data Hiding Architecture with Text Pattern Authentication and Verification. In that he proposed Security of hidden data is a tradeoff between capacity, robustness and embedding against induced distortion. He used the fourth parameter, authentication and verification. Authors have used 128-bit Advanced Encryption Standard (AES) for encryption and Least Significant Bit (LSB) algorithm to hide textual data behind Bitmap images. Selected images by user can be transformed into text pattern and then used for authentication and verification or as hidden message. The password protection mechanism is supported at both the stages of encryption and data hiding respectively to provide better security. The present paper claims the superiority of the designed model over existing one in terms of combined security provided by its robust authentication / verification system, encryption and data hiding.

In 2008, Zhicheng Ni, Yun Q. Shi [9] proposed Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication. In that he proposed among various data hiding techniques, a new subset, lossless data hiding, has received increasing interest. Most of the existing lossless data hiding algorithms are fragile in the sense that the hidden data cannot be extracted out correctly after compression or other incidental alteration has been applied to the stego-image. The only existing semi-fragile (referred to as robust in this paper) lossless data hiding technique, which is robust against highquality JPEG compression, is based on modulo-256 addition to achieve losslessness. he proposed a novel robust lossless data hiding technique, which does not generate salt-andpepper noise.

In 2001, Chun-Shien Lu and Hong-Yuan Mark Liao [10] proposed a novel multipurpose watermarking scheme. In which robust and fragile watermarks are simultaneously embedded, for copyright protection and content authentication. By quantizing a host image’s wavelet coefficients as masking threshold units for two complementary watermarks are embedded using cocktail watermarking and they can be blindly extracted without access to the host image. For that purpose of image protection, the new scheme guarantees that, no matter what kind of attack is encountered, at least one watermark can survive well. On the other hand, for the purpose of image authentication, our approach can locate the part of the image that has been tampered with and tolerate some incidental processes that have been executed. This output is shows how that the performance of our multipurpose watermarking scheme is indeed superb in terms of robustness and fragility.

Author & year	Paper title	Technique used	Advantages	Disadvantage
Feng Wang & Won-Li-Lyu,Jeng Shyang-Pan, 2016	Robust image authentication scheme with self-repair capability for gray scale source document images via PNG format	Image authenticati on and data repairing	It can resist the attacks	---
Patel Roshani, Prof Aslam Durvesh,etl, 2015	Data Hiding In Encrypted Image	Image encryption algorithm	Secretly embedding a message into the data	Grayscale via PNG format image is not used
K.V.Arya & Akanksha Bandil, 2014	An Improved Image Authentication Technique using Random-Sequence based Secret-Sharing Scheme	Image authenticati on and data repairing	Grayscale PNG format image used and data is self-repaired	Attacks cannot be resist
Che-Wei-Lee & Wen Hsiang Tsai,2012	A Secret-Sharing-Based Method for Authentication of Gray scale Document Images via the Use of the PNG Image with a Data Repair Capability	Image verification and data hiding	Protecting the security of the data hidden in the alpha channel	Image cannot resist self-substitution attack and the same position substitution attack or cut off attack
Meng Guo& Hangbin Zhang,2010	High Capacity Data Hiding for Binary Image Authentication	Image Quality Assessment	Data hiding scheme with high capacity for binary images	Can't repair the data which is hidden.
Nabin Ghoshall, J. K. Mandal, etl,2009	Image Authentication by Hiding Large Volume of Data and Secure Message Transmission Technique using Mask.	IAHLVDS MTTM algorithm	Secures message transmission technique by embedding message/image into color images.	Data is not repaired
Chin-Chen Chang,Wei-Liang Tai&Kuo-Nan Chen,2008	A Lossless Data Hiding Based on Histogram Modification for Image Authentication	Lossless data hiding algorithm	Lossless Data Hiding Based on Histogram Modification for Image Authentication used	---

Author & year	Paper title	Technique used	Advantages	Disadvantage
Ankur Dauneria, Kumari Indu,2008	Encryption Based Data Hiding Architecture with Text Pattern Authentication and Verification	Steganographic algorithm	The password protection mechanism is supported at both the stages of encryption and data hiding	It requires more time to compare Images
Zhicheng Ni, Yun Q. Shi, 2008	Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication	Robust lossless image data hiding algorithm	The robust lossless data hiding algorithm can be readily applied in the medical field, law enforcement remote sensing	It does not generate salt-and-pepper noise
In 2001, Chun-Shien Lu and Hong-Yuan Mark Liao,2001	Multipurpose Watermarking for Image Authentication and Protection	Multipurpose watermarking algorithm	image authentication and protection	Tampering of images

4. CONCLUSIONS

To reiterate, paper represents different authentication techniques offered by the researchers, which are mainly classified into digital signature based, watermarking based, transform domain based and other authentication techniques with data repair capability. It is essential that the information represented is immune to the different kind of manipulations to some extent. Much of the future work can be done to develop efficient and robust techniques for image authentication with data repair capability for color images. Moreover, these techniques are not only limited to grayscale images but also can be applied on color images and videos.

REFERENCES

[1] Feng Wang & Won-Li-Lyu,Jeng Shyang-Pan proposed a “Robust image authentication scheme with self-repair capability for gray scale source document images via PNG format”,IET image process,2016 processing,vol.21,No.1,January 2012.pg. no. 207-218.

[2] Patel Roshani, Prof Aslam Durvesh, etl proposed “Lossless Method for Data Hiding in Encrypted Image”,2015, IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems

[3] K.V.Arya & Akanksha Bandil proposed“An Improved Image Authentication Technique using Random-Sequence based Secret-Sharing Scheme”,Arya 2014.

[4] Che-Wei-Lee & Wen Hsiang Tsai proposed” A SecretSharing-Based Method for Authentication of Gray scale Document Images via the Use of the PNG Image With a Data Repair Capability”,IEEE transactions on image

[5] Meng Guo& Hangbin Zhang proposed "High Capacity Data Hiding for Binary Image Authentication", 2010 I international Conference on Pattern Recognition. IEEE computer society, pg. no.1441-1444.

[6] Nabin Ghoshall, J. K. Mandal, etl. Proposed" Image Authentication by Hiding Large Volume of Data and Secure Message Transmission Technique using Mask,2009, pp.1103- 1108

[7] Chin-Chen Chang, Wei-Liang Tai&Kuo-Nan Chen proposed a" Lossless Data Hiding Based on Histogram Modification for Image Authentication", 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous computing.pg no. 506-511

[8] Ankur Dauneria, Kumari Indu proposed" Encryption Based Data Hiding Architecture with Text Pattern Authentication and Verification", IEEE 8th International Conference on Computer and Information Technology Workshops, pg.no. 236-241.

[9] Zhicheng Ni, Yun Q. Shi proposed"Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication" IEEE Transactions on circuits and systems for video technology,vol.18,No.4,April 2008,pg no.497-512

[10] Lu, C.S., Liao, H.Y.M.: 'Multipurpose watermarking for image authentication and protection', IEEE Trans. Image Process., 2010, 10, pp. 1579–1592