A Review Paper on Image Authentication with Data Repair Capability

Arjun Nichal, Dr. Bhalchandra Godbole

Abstract— Image Authentication technique has gained importance in now days. The digital revolution in Image Processing has made it possible to create manipulate and transmit digital images in a simple and fast manner. Therefore most of the important images such as military, Medical, Companies secret data must be protected against manipulation. So to protect originality and authenticity of multimedia images and important scanned documents various authentication methods are evolved. Mainly these methods comprise conventional copyright, fragile watermarking based, Semi Fragile Watermarking based and digital signature based on image content. These all above methods are categorized into service they provide. Tamper detection, Robust to various image processing operations and data repair capabilities these are the services. This survey paper is based the methods that are used for image authentication with data repair capability.

Index Terms— Image Authentication, Data Repair Capability, Watermarking, Tamper Detection, Alpha Channel, Data Hiding, Embedding.

1 Introduction

Authentication is the process or action of verifying the identity of user or process. Image Authentication have recently gain great attention due to its imporatance of large number multimedia applications. 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 that 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 thebinary version image, we randomize it by using exclusive-or method with a random binary sequence generated by the secretvalue 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.

General Objectives of Image Authentication System

Before discussing various methods, we start with the general

- *Arjun Nichal is currently pursuing Ph. D in Electronics & Telecommunication engineering in Shivaji University Kolhapur, India, working as a Assiatnt Professor in Adarsh Institute of Technology & Research Centre, Vita, India. E-mail: arjunnichal@gmail.com*
- *Dr. Bhalchandra Godbole is currently working as an Associate Professor in KBP College of Engineering Satara, India. E-mail: bbgodbole@rediffmail.com*

Objectives of the authentication system study.

1. Sensitivity:
The authentication system must be able to detect any modification in a digital image or scanned documents. Detection of any kind of modification is required.

2. Localization: The main objective of authentication system is to localize altered region in an image. The system able to detect tampered region.

3. Recovery:
The authentication system must be able to recover tampered data partially or completely.

4. Robustness:
Authentication System must be robust in some of the image authentication applications. This objective is only valid for selective authentication service.

5. Security:
Authentication system must have the capability to protect authentic data against malicious attacks.

6. Complexity:
The authentication system must run for various real time applications. So these systems should neither complex nor slow.

2 Basic Methodology

In Authentication Sender and Receicver plays most imporatant role. The following figure shows us basic methodology.

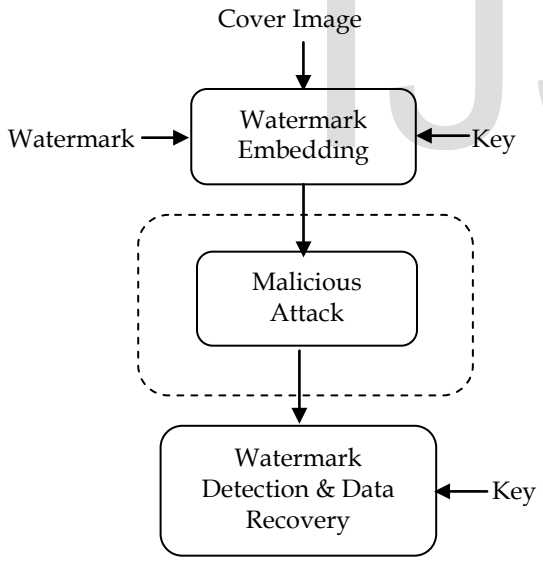

Fig. 1. Basic Methodology of Image Authentication System

This is a basic methodology. Watermark embedding is carried out in cover image. If somebody tamper the image then at the receiver end after watermark extraction we can found whether cover image is authentic or not.

If (Received watermark ~ = Original Watermark)
Statement = Manipulation Occurs.
else
Statement = Manipulation Not Occurs.
end

3 Literature Review

Some authors proposes various image authentication techniques based on image authentication with data repair capability.

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, et al [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 Random-Sequence 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.

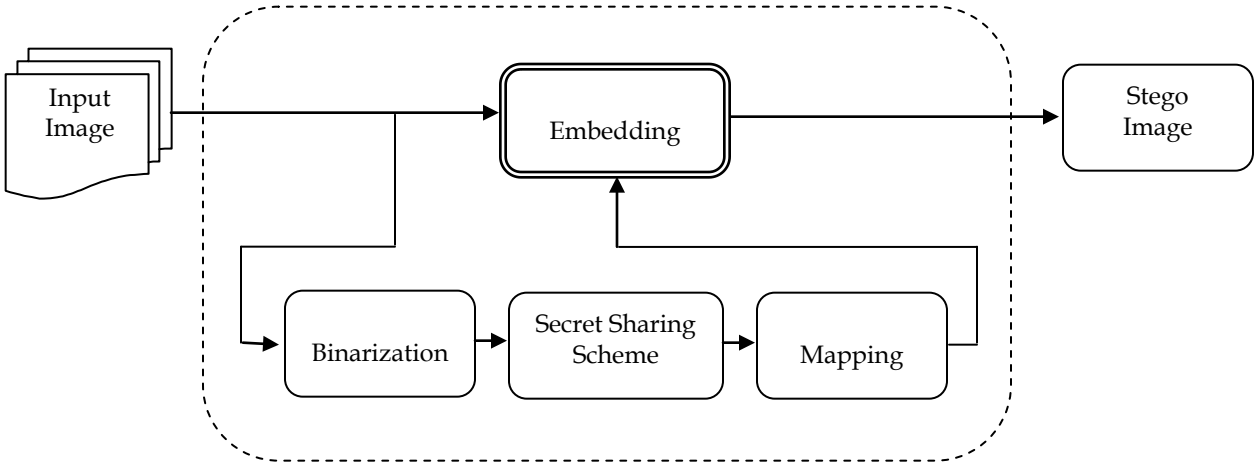

Fig. 2. Image Authneitcation based on binarization and secrete sharing scheme.

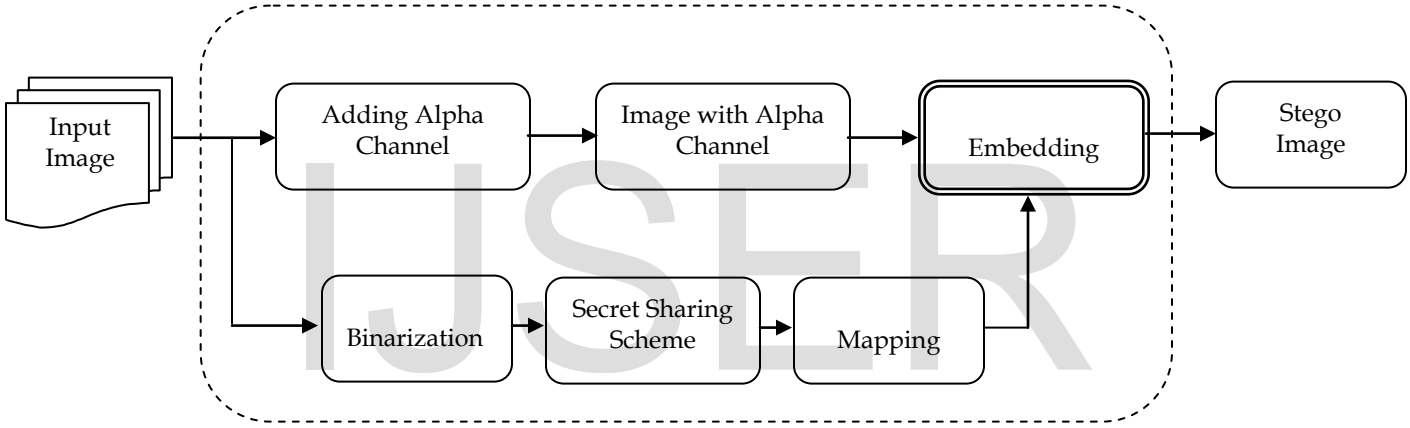

Fig. 3. Image Authneitcation based on Embedding Authentic Data in Alpha Channel.

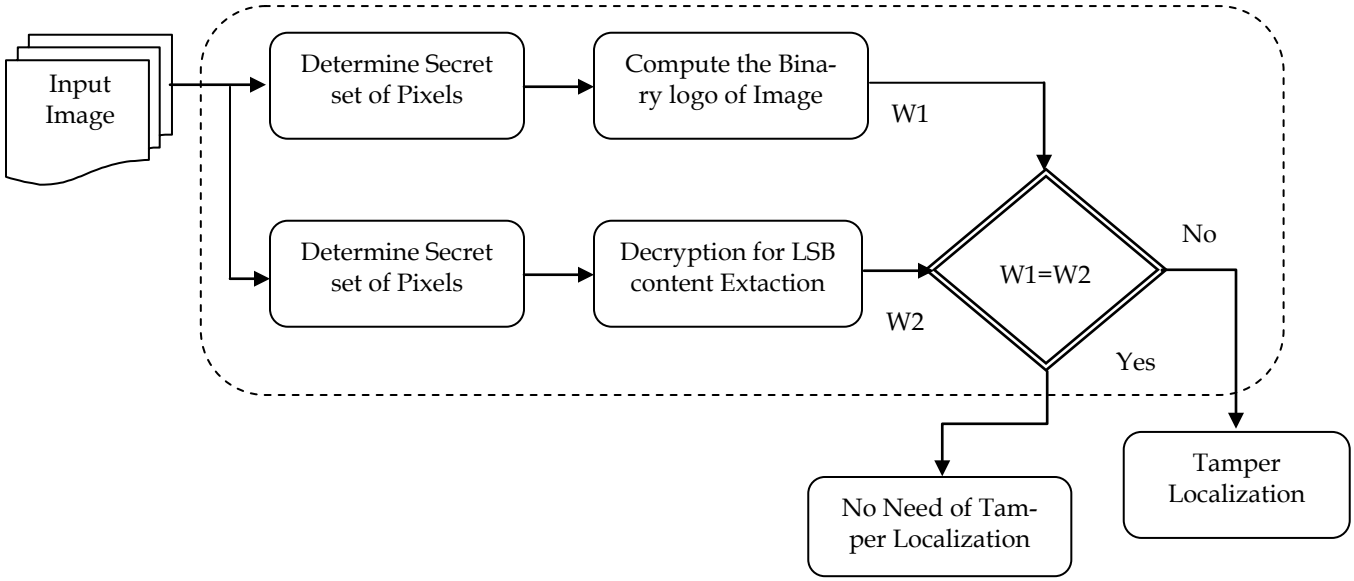

Fig. 4. Image Authneitcation with Tamper Localization based on Spatial Domain.

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 amount 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 present 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 present 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 high-quality 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-and-pepper 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.

The comparison table of all methods by different authors is attached in appendix 1 (at the end of the paper)

4 CONCLUSION

This literature review reveals the fact that there are different methods of Image Authentication with data repair capability. Some methods are based on fragile watermarking, some are belongs to semi – fragile watermarking, some are based on spatial domain embedding, some are based on alpha channel embedding. Image authentication methods with transform domain are highly robust. Spatial domain based embedding authentication methods are very sensitive. Now days there is huge scope of image authentication methods with data repair capabilities. The objectives of authentication need to fulfill by new algorithms. Tampering detection, localization and data repair capabilities have to introduce in new algorithms. Robustness need to maintain as per application demand. Need to maintain high Visual quality of authentic image after data embedding

ACKNOWLEDGMENT

I would like to express my deep snese of gratitude to my guide Dr. Bhalchandra Godbole for their valuable guidance, encouragement and kind co-operation throughout this study. I also express my thanks towords Rayat Institute of Research & Development (RIRD) Satara, India for making all the facilities available to us and fulfils all my requirements.

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 Secret-Sharing-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 Processing, Vol. 21, No. 1, January 2012*

[5] Meng Guo& Hangbin Zhang proposed "High Capacity Data Hiding for Binary Image Authentication", 2010 *Iinternational 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

Appendix 1

Table 1. Literature Survey comparison table by different Authors

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 authentication and data repaired	It can resist the attacks.	Color image is not used.
Patel Roshani, Prof Aslam Durvesh,etl, 2015	Data Hiding In Encrypted Image.	Image authentication	In that message is secretely embed into 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 authentication and data repaired	In that Grayscale PNG format image usea and data is self repaired.	In that 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 authentication and data repaired	In that Grayscale PNG format image usea and data is self repaired.	In that attacks cannot be resist.
Meng Guo& Hangbin Zhang,2010	High Capacity Data Hiding for Binary Image Authentication.	Image Quality Assesment	In that the data hiding scheme with high capacity for binary images.	Data is not repaired.
Nabin Ghoshall, J. K. Mandal, etl,2009	Image Authentication by Hiding Large Volume of Data and Secure Message Transmission Technique using Mask.	LAHLVDSMTTM algorithm	It 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	In that Lossless Data Hiding Based on Histogram Modification for Image Authentication used.	Data is not repaired.
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.	PNG format image is not used. Data is not repaired.

Author & year	Paper title	Technique used	Advantages	Disadvantage
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.	Data is not repaired.
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.