www.ijaceeonline.com ISSN: 2456 - 3935

International Journal of Advances in Computer and Electronics Engineering
Volume 4, Issue 7, July 2019, pp. 1–6

Review on Digital Image Watermarking Techniques to Shares Secure Image

Abu Saleh Musa Miah
Lecturer, Department of Computer Science and Engineering, Bangladesh Army University of Science and Technology (BAUST), Bangladesh
Email: abusalehcse.ru@gmail.com

Salma Masuda Binta
UG Scholar, Department of Electrical and Electronics Engineering, Bangladesh Army University of Science and Technology (BAUST), Bangladesh
Email: salmamasudabinta@gmail.com

Abstract: *The newest analysis trends in digital image watermarking are covered transient study, concerning a number in this paper. High quantity of data or terribly sensitive information is carried in the sensitive images of the photographs. For the watermarking, the employment of sensitive pictures, the growing space of analysis for data exchange is increasing. Since it provides numerous edges whereas handling sensitive pictures. Throughout the transmission, the sensitive pictures can be a victim of a change of state. Detection of any reasonably change of state throughout the transmission is known as image authentication. This is extremely needed for these pictures. We've studied concerning recovery approaches and a number of the newest tamper detection in this paper. We've also studied some of the watermarking approaches.*

Keyword: *Detection; Sensitive images; Tampering; Image authentication formatting; Visual cryptography;*

1. INTRODUCTION

A mechanism for the copyright protection of transmission content is known as watermarking. A process which is used to embed some copyright info or helpful information into various transmission content like video, image or audio is known as the watermarking process. Watermarking is a combination of cryptography and image processing. Handling of transmission contents like pictures Visual Cryptography performs much better. The protection for these contents can be done by Visual Cryptography. On the retrieval of those contents it puts some constraints. Higher protection level can be achieved by Visual Cryptography.

The most important sources of data increasing are the utilization of transmission contents together. It is possible with the recent development of information technology. For an oversized quantity of multimedia content, a varied function is transferred from one finish to another. For these contents, the protection of the copyright is a major issue. To embed the useful information into some sensitive transmission contents like medical pictures is very useful. Additionally, it creates a higher utilization of this process. Handle the sensitive pictures is the largest problems for watermarking as the transmission of those sensitive pictures is increasing. The security for these contents is the burning question. So, the most important thing is to do the copyright protection. The biggest challenge for watermarking is the changes in original contents. This change should remain as low as possible. Additionally, it should be reversible. To create strong watermark against different attacks damages protection is also important. They may be a victim of some intentional meddling. Because these contents carry sensitive information it is a serious issue for the correct detection of tampering. The details of watermark like its sort are In Section II. Some common attacks on watermark and their characteristics are mentioned and performance parameters of some basics of VC are additionally explained. This also contains the reviews of some recovery strategies and existing Tamper Detection with the application of Visual Cryptography. Watermarking is in Section III. Tabular comparison between these strategies and finally we've concluded this paper is covered in Section IV.

2. EASE BASICS OF VISUAL CRYPTOGRAPHYAND WATERMARKING

The watermarking technique is divided into following major sorts based on some characteristics

A. Watermark Embedding Domain

i. *Spatial Domain Watermarking:* Manipulation

Cite this paper:

Abu Saleh Musa Miah, Salma Masuda Binta, "Review on Digital Image Watermarking Techniques to Shares Secure Image", International Journal of Advances in Computer and Electronics Engineering, Vol. 4, No. 7, pp. 1-6, July 2019.

with the image element is described in this method. With the watermark bit, some bits from the element price is modified.

ii. *Remodel Domain Watermarking:* Some variety of transformation of the initial image is used in this way. Some samples of these transformations are distinct circular function remodel (DCT), distinct moving ridge remodel (DWT) etc.

B. Perceptibility in step

iii. *Visible:* If the embedded watermark is clear in nature, it'll be visible in human vision.

iv. *Invisible:* The Licensed user is allowed to recover the embedded watermark that is onerous to spot by human vision.

C. Hardiness of Watermark

i. *Fragile:* Towards any quite modification within the transmission content the delicate watermarks are sensitive. The detection of any style of change of state to the initial transmission content is used by this process.

ii. *Sturdy:* The watermark is able to survive when some international or uninternational attacks. Watermarks are wont to engraft copyright data for Watermark Acquisition the requirement of supply information are

- *Blind:* For watermark extraction, the initial unwatermarked supply information must be there.
- *Semi-Blind:* This Watermark desires some options of the initial supply information. Additionally to precise the watermark.
- *Non-Blind:* Non-Blind Watermark doesn't like any quite supply information for the extraction.

It's possible to face varied attacks throughout the transfer method of watermarked content. Some common attacks that a watermarked content will make sure that you have the correct template.

A. Watermark Removal

To get rid of or injury of the watermark information the watermark removal could be a quiet attack. There are varied doable strategies to perform this attack for this.

i. *Cropping:* In the watermarked image to get rid of or injury the watermark cropping is performed. The cropped region might contain some watermark bits, in spatial domain watermarking, this is often a lot of harmful.

ii. *Noise:* The addition of noise is also intentional or unintentional in the watermarked image. It'll also injury the initial watermarked pixels furthermore as pixels.

iii. *Filtering:* Various filters are accessible [18] like a median filter, sharpening filter or Blurring filter. On the watermarked image, these filter may perform completely different effects. It has an effect on the image quality also.

B. Geometric Transformations

Geometric transformations might lead to broken watermark in the watermarked image.

i. *Translation:* With the employment of some translation matrix the interpretation referrers to the linear remodel of the image coordinates.

ii. *Rotation:* Concerning some reference axis the image is turned by some angle.

iii. *Scaling:* With relation to some predefined scaling issue the elements of the image are scaled up or scaled down.

iv. *Cutting:* The transformation during the worth of 1 axis of image element is unbroken fastened and different values are altered is shearing.

C. User fixed Processing

The example of this types of attack is when a few malicious users purposely meddling the image. The meddling isn't visible by human eyes.

D. Compression

Since the web is the largely used medium for information exchange, the photographs are sent using web too. Throughout transmission, the compression [19] is performed so as to cut back the scale of the image. One of the renowned compressions customary used is JPEG 2000. The injury to watermark is one of the unwanted aspect effects of the compression. So against, such compressions, the watermark has to be strong enough to survive.

It depends on the character of the multimedia system content (General or Sensitive). The performance of the watermarking mechanism is accustomed to some parameters which live use. Below there are some widely used parameters.

Peak ratio (PSNR): Transparency of the watermarked image with regard to original image will be measured by the PSNR price the sensory activity.

Bits-Per-Pixel (BPP): The quantity of watermark information embedded within the original image is employed to calculate by the bits-per-pixel.

Normalized Correction (NC): The extracted watermark will be calculated using North Carolina by the similarity between the initial watermark. Against varied attacks, it measures the lustiness of the watermark.

Visual Cryptography: Naor and Shamir 1st planned the idea of Visual Cryptography in 1995 [17]. During this time several analysis has been disbursed. To urge the initial image back the plan is to divide the image into a range of shares and a few pre-defined numbers of shares are needed.

3. EXISTING WORK REVIEW

3.1Tamper Detection and Recovery (Authentication of Image)

In daily life, using the internet, sensitive pictures are being transferred. To find and, in some case, recover the change of state, there are varied mechanisms.

A twin watermark mechanism for recovery of image change of state and detection was planned by Lee and designer [1], in 2008. A block-based watermarking technique was planned by them. For every non-overlapping block of the image, they took 2 copies of the watermark. For the detection of a change of state, verification is employed within the planned theme. A public chaotic commixture algorithmic program and a secret key and are accustomed for actual the watermark that gives the tamper recovery in case of tampering. In case ninetieth of the change of state, the theme will recover up to some extent. It's a Blind Watermark Mechanism. Some attacks like covering, cropping, exchange and removing this mechanism are very strong. Since 2 copies of the watermark are embedded, the number of the payload is clearly high. For Tamper detection, a semi-fragile watermarking mechanism [2] was planned by Radu O. Preda in 2012. Discreet riffle rework (DWT) was used in this rework domain watermarking. With the assistance of a secret key random permutation of wavelet coefficients is completed. Against some native attacks, this secret key protects the watermark.

A recovery mechanism and DCT based mostly image tamper detection were planned by Qingfan Zhang, Junpeng Zhang and Hongli fifty-five [3] in 2012. The DCT coefficients of every block are encoded in this block-based watermarking theme. This is embedded because of the watermark into another block. For enhances of the safety level, the non-linear chaotic sequence is employed in block mapping.

In 2013 a recovery approach for medical pictures and tamper detection was done by Adiwijaya et al. [4]. In ROI using Huffman compression insert the watermark for tamper detection, original image LSB are watermarked in RONI. For the ROI the aforesaid Approach is reversible. A thousandth correct is concerning for the detection of a change of state. For a few attacks, the recovery rate is about ninety-eight.

A reversible image authentication mechanism was planned in 2014 by Yu-Chen Hu and Chun-chi Lo [5]. The aforesaid approach is block based mostly watermarking approach. This aforesaid approach maintains the great watermarked image quality. This process is reversible. So, the aforesaid approach can be applied to sensitive pictures. For tamper detection from Holy sacred writing, a two-layer fragile watermarking technique was planned in 2014, by Khalil et al. [13]. As spatial domain watermarking the 2 layers watermarking includes reworking. Firstly the riffle coefficients are watermarked. For embedding another watermark, the LSB from the spatial domain is manipulated then. Whether or not the tampered space is extremely tiny the planned technique will find tamper.

A color image authentication theme was planned by Chen, Tang, and Hsieh [14]. The higher visual quality of the watermarked image can be gained by this approach. in 2014, a picture authentication theme for medical pictures was planned by E. Sreenivasa Reddy and R. Eswaraiah [15]. At the border pixels, the watermark information is embedded. Additionally, as details of the ROI, the watermark data includes authentication codes. At the receiver finish, the correct recovery for ROI is feasible.

3.2 Image Watermarking and Visual Cryptography

The utilization of VC for watermarking is wise for contents like pictures because the Visual Cryptography provides security too. To firmly enter image because of the watermark Visual Cryptography is suitable. For the watermarking purpose, VC is employed in (2,2). Some review of the analysis works which have an application of VC in the space of Image Watermarking is as follows.

A VC mechanism for watermarking was planned In 2007, by Tso, Lou, and Liu [6]. The DWT of the duvet image was used by them. This generates the general public and secret share key. With the Certified Authority (CA) the key share is registered. Between these 2 stacks, the XOR operation can result in a watermark image. An approach supported Multi-Pixel secret writing technique (MPM) was planned bt Tu associated Hsu [7]. The watermark is separated publicly in this. Private share and personal shares are commanded by the owner. In the image, the general public share is embedded. This is possible because the watermark supports the embedding algorithmic program. The approach has physical property and higher hardiness.

A semi-blind watermarking technique was planned by B Surekha and GN Swamy [8]. In this technique the XOR-based mostly VC is employed. Within the image, the first watermark is not embedded. A secret share and a public share in the DWT of the quilt image is employed. The key share is kept to a trusty third party. For enhance the protection, these keys are accustomed to generating public share and the secret. A twin watermarking algorithmic program was given by Han, He and dynasty [9] in 2013. Twin watermarking algorithmic program supported VC for color pictures. The aforementioned approach makes use of DWT of the quilt image. The embedding capability improves by the planned algorithmic program.

TABLE I. REVIEW METHODS SUMMARIZATION

Method/ Approach	Summarization			
	Tamper Detection	Temper Recovery	Watermark Physically Embedded	Remarks
[1]	Yes	Yes	No	To induce the second probability for recovery, two copies of watermarks are supplementary. Amount of payload is higher.
[2]	Yes	No	Yes	Watermarking provides Tamper localization. Image quality is comparatively higher.
[3]	Yes	Yes	Yes	For Image Authentication, DCT coefficients are used. Higher i.e. about 80%.
[4]	Yes	Yes	Yes	On medical pictures, the focus is on. From the image is an essential purpose for the separation of RONI and ROI. Recovery and the detection rate is incredibly high.
[5]	Yes	No	Yes	For watermarking, the theme uses a technique called Prediction-Based Histogram Shifting. The method is reversible when it is applied to sensitive pictures.
[6]	No	No	No	The idea of the public and personal watermark is applied. To retrieve original watermark the XOR primarily based rules are accustomed.
[7]	No	No,	Yes	Visual cryptography is used in this approach that improves the strength of the watermark.
[8]	No	No	No	Standard of the retrieved watermark is higher.
[9]	No	No,	Yes	Two watermarks are extra mistreatment rework domain watermarking. On the second watermark, the visual cryptographic ideas are used.
[10]	No	No,	Yes	When watermark retrieval is needed 1st share is dynamically constructed.
[11]	No	No,	Yes	Against flipping and rotation attack the planned approach is strong. Hardiness of the watermark can be increased by the use of feature metrics.
[12]	No	No	No	For encoding, the lossless codebook is planned.
[13]	Yes	No	Yes	The little amount of tampered space is achieved.
[14]	Yes	No	Yes	For color pictures approach projected. The watermark is very sturdy.
[15]	Yes	For	Yes	Approach for ROI space is achieved.by accurate recovery.

A VC was planned in 2013, by Wang, Maya Lin, and principle [10]. It was based on mostly image authentication approach. When following some predefined steps, one of the images is generated from the general public image. The shared one and secret image i.e. watermark are accustomed to generating the share of a pair. The secret image is extracted exploitation by the visual cryptography rules.

A method for copyright protection for high dimensional pictures was planned in 2014, by B Surekha and GN Swamy [11]. For possession share generation, the theme obtains the feature metrics. This is registered with the third party. The general public share is generated exploitation for watermark extraction. XOR-based mostly VC is performed and the feature metrics dynamically to come up with the watermark. A lossless codebook based mostly approach for watermarking was given in 2014, by Park, Kim and Yoo [12]. They planned AN improved codebook for watermarking in this. Boolean AND, OR operation for watermark extraction was used in this process. Against numerous image, process attacks the aforementioned theme is powerful.

We've got summarized the strategies mentioned here up to now in table-I. The characteristics of every approach and therefore the remarks for the approach is included in this report.

4. CONCLUSION

The watermarking analysis for sensitive pictures typically targets fragile and strong watermarking. The detection of a change of state is crucial for these images. As a watermark, it has a higher degree of lustiness against numerous image process attacks that are accustomed to carrying important info. The algorithms used for the sensitive image, watermarking should guarantee minimum doable quantity of payload. The precise recovery of the first image when watermark removal is crucial

Since the number of transmission contents for info exchange is increasing, the requirement for Digital Image Watermarking is increasing day by day. The protection of watermark is additionally increasing. The employment of visual cryptography for its many benefits that create it appropriate for watermarking. during this paper. Regarding a number of the analysis trends in recent years, we've got given a transient introduction that targets Image Authentication. It'll be useful for analysis United Nations agency do research in image watermarking and visual cryptography because the review contains the latest works during this space.

REFERENCES

[1] T.Y.Lee,S.D.Lin, “Dual watermarking for image tamper detection and recovery,” *Pattern Recognitin,* vol.41, no.11, pp. 3497-3506,2008

[2] Preda, Radu O, “Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain.” *Measurement,* vol. 46,no.1,pp.367-373,2013.

[3] Zhang, Junpeng, Qingfan Zhang, ad Hongli Lv, “A novel image tamper localization and recovery algorithm based on watermarking technology.” *Optik-International Journal for Light and Electron Optics,* vol.124,no.23,pp.6367-6371,2013.

[4] Adiwijaya, Faoziyah, Permana, Wirayuda, Wisesty, “Tamper detection and recovery of medical image watermarking using modified LSB and Huffman Compression,” In Proc.,ICIA,pp.129-132,2013.

[5] Lo, Chun-Chi, and Yu-Chen Hu. “A novel reversible image authentication scheme for digital images.” *Signal Processing,* vol. 98, pp.174-185,2014.

[6] Lou, Der-Chyuan, Hao-Kuan Tso, and Jiang-Lung Liu. “A copyright protection scheme for digital images using visual cryptography technique,” *Computer Standards & Interfaces,* vol. 29,no.1,pp.125-131,2007.

[7] Tu,Shu-Fen, and Ching-Sheng Hsu. “Digital Watermarking Method Based on Image Size Invariant Visual Cryptographic Scheme.” In *Ubiquitous, Autonomic and Trusted Computing,2009. UIC-ATC’09.Symposia and Workshops on,*pp. 362-366.IEEE,2009.

[8] Surekha,B., and G.Swamy. “A semi-blind image watermarking based on Discrete Wavelet Transform and Secret Sharing.” In *Communication, Information & Computing Technology (ICCICT),2012 International Conference on,*pp. 1-5.IEEE,2012.

[9] Han, Yanyan, Yixiao Shang, and Wencai He. “DWT-Domain Dual Watermarking Algorithm of Color Image Based on Visual Cryptography .” In *Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference on,* pp. 373-378.IEEE, 2013.

[10] Wang, Yuh-Rau, Wei-Hung Lin, and Ling Yang. “A lossless watermarking using visual cryptography authentication.” In *Machine Learning and Cybernetics (ICMLC),2013 International Conference on,*vol.3, pp.1109-1113.IEEE,2013.

[11] Gavini, Narasimha Swamy, and Surekha Borra. “Lossless watermarking technique for copyright protection of high resolution images.” In *Region 10 Symposium, 2014 IEEE,*pp. 73-78. IEEE,2014.

[12] Park, Geum Dal, Dea Su Kim, and Kee Young Yoo. “Lossless Codebook-Based Digital Watermarking Scheme with Authentication.” In *Information Technology: New Generations (ITNG),2014 11th International Conference on,*pp. 301-306.IEEE, 2014.

[13] Khalil, Mohammed S., Fajri Kurniawan, Muhammad Khurram Khan, and Yasser M. Alginahi. “Two-Layer Fragile Watermarking Method Secured with Chaotic Map for Authentication of Digital Holy Quran.” *The Scientific World Journal vol.* 2014, doi:10.1155/2014/803983, 2014.

[14] Chen, Chun Hung, Yuan Liang Tang, and Wen Shyong Hsieh. “ Color Image Authentication and Recovery via Adaptive Encoding.” In *Computer, Consumer and Control (IS3C), 2014 International Symposium on,* pp. 272-275.IEEE,2014.

[15] Eswaraiah, Rayachoti, and E. Sreenivasa Reddy. “Medical Image Watermarking Technique for Accurate Tamper Detection in ROI and Exact Recovery of ROI.” International Journal of telemedicine and applications vol. 2014, doi:10.1155/2014/984646,2014.

[16] Tsai, Piyu, Yu-Chen Hu, and Hsiu-Lien Yeh. “Reversible image hiding scheme using predictive coding and histogram shifting.” *Signal Processing, vol.* 89,no.6,pp. 1129-1143, 2009.

[17] Naor, Moni, and Adi Shamir. “Visual cryptography.” In *Advances in cryptology-EUROCRYPT’94,* pp. 1-12. Springer Berlin Heidelberg, 1995.

[19] http://en.wikipedia.org/wiki/JPEG_2000.

Authors Biography

Abu Saleh Musa Miah, is a Lecturer of Department of CSE in a University. He completed his B.Sc.Engg and M.Sc.Engg In CSE department at University of Rajshahi, Bangladesh. His research interests are artificial intelligence,Brain Computer Interfacing, EEG Signal, Computer Vision, Satellite Image.

Salma masuda binta, is a B.Sc.Engg student in department of EEE at Bangladesh Army University of Science and Technology. She is an associated member of IEEE (Membership No-94181799). Her research interests are artificial intelligence, Brain Computer Interfacing, EEG Signal, Computer Vision, Satellite Image

Cite this paper:

Abu Saleh Musa Miah, Salma Masuda Binta, "Review on Digital Image Watermarking Techniques to Shares Secure Image", International Journal of Advances in Computer and Electronics Engineering, Vol. 4, No. 7, pp. 1-6, July 2019.