ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

IJIREEICE INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 7, July 2015

A review on multiple Watermarking techniques in digital photography for Image authentication and encryption

Mukesh Kumar Tripathi[1], Pradeep Kumar Nathaney[2], Vinith Chauhan[3]

M.Tech, Digital Communication, SMEC, Neemrana, India[1]

Assistant Professor, Electronics, SMEC, Neemrana, India[2]

H.O.D, Electronics, SMEC, Neemrana, India[3]

Abstract: A digital watermark is an invisible signature embedded inside an image to show authenticity and ownership. To avoid obstruction of the original image effective digital watermark must be perceptually imperceptible. It should be statistically invisible to prevent detection, and it should also be robust to many image manipulations, such as filtering, additive noise, and compression. Digital watermarking has been invented and researched as a novel, unconventional method to implement the logical possessions privileges and defend digital media from tampering. It consists of a process of embedding into a mass signal a perceptually visible digital signature, message communication.
In the proposed watermarking system, the discrete wavelet transform (DWT) is used for embedding watermarks and watermark is generated from the content of the original image and, as it is aclearanalysis technique for evaluatingtime-frequency, which can be well improved for extracting the information pleased of the image.

Index Terms: Digital Watermarking, Amold Transform, Transparent Digital Signature, Discrete wavelet transforms (DWT)

I. INTRODUCTION

The web is a fabulous dissemination framework for the advanced media on account of its reasonability and productivity. Additionally the pictures could be promptly imparted, effortlessly utilized, transformed and transmitted which causes genuine issues, for example, unapproved utilization and control of computerized substance. Therefore, there is the requirement for verification strategies to secure advanced pictures. Computerized watermarking is a procedure which installs extra data called advanced mark or watermark into the advanced substance so as to secure it. A watermark is a shrouded indicator added to pictures that might be located or concentrated later to make some insistence about the host picture [1].

The significant purpose of computerized watermarking is to discover the parity among the viewpoints, for example, heartiness to different ambushes, security and intangibility. The invisibleness of watermarking strategy is focused around the force of implanting watermark. Better invisibleness is attained for less power watermark. So we must select the ideal power to insert watermark. All in all there is a little tradeoff between the implanting quality (the watermark strength) and quality (the watermark imperceptibility). Expanded heartiness obliges a stronger inserting, which thus builds the visual corruption of the pictures. For a watermark to be viable, it ought to fulfill the accompanying peculiarities [2]. They are as follows:

- ***Imperceptible*** **-** It must be perceptually obscure so that quality of image is not degraded and attackers are prohibited from deleting and resultit. A watermark is known asinvisible if the watermarked data is perceptually equivalent to the original, un-watermarked image.
- ***Extractable*** **-** The autonomous control authority or data owner should easily extract it.
- ***Unambiguous*** **-** The watermark recovery should unambiguously recognize the data owner.
- ***Robustness*** **–** Robust watermarks could be used in piracy protection and privacy applications to secure from copy and access manage data.It mustallow some of the mutual image processing attacks. A watermark is known as robust if it attacks a selected class of conversions.

The digital image watermarking scheme can be divided into two categories. They are visible digital image watermarking and invisible image watermarking techniques. In detectable watermarking, the data is perceptible in the image or video. Usually, the data is any text or an image which acknowledges the owner of the innovative document. In undetectable watermarking, data is appliedor encrypted as digital data to audio, image or video, but it cannot be apparent as its original content [3].

Further, the imperceptible watermarks are sorted into watermarking strategies as subtle and robust. Normally, a strong imprint is for the most part utilized for proprietorship distinctiveand copyright protection on the grounds that they are intended to withstand attacks, for example, basic picture transforming operations, which endeavor to evacuate or reduce the watermark. These algorithms assured that the embedded watermark signal cannot be deleted by image processing operations. Though a subtle or semi-subtle watermark are predominantly connected to data confirmation and integrity check on the grounds that they are extremely touchy to attacks, i.e., it can identify slight changes to the watermarked image with high possibility. This exploration manages a robust

DOI 10.17148/IJIREEICE.2015.3720

watermarking. The normally utilized watermarking applications incorporate copyright related applications and military applications and data validation applications [4].

II. DIFFERENT WATERMARKING TECHNIQUES

A few strategies have been proposed in writing. Xie L. et. al. Proposed new space methods of digital watermarking. Two classes of Digital watermarking algorithms are spatial-area procedures and recurrence space methods. Slightest Significant Bit (LSB) is the least difficult procedure in the spatial area strategies which straightforwardly adjusts the intensities of some chose pixels. The recurrence area system converts a picture into a set of recurrence space coefficients. [5]

R. Ramanaet. al, proposed watermark coefficients. The change received may be discrete cosine convert (DCT); discrete Fourier converts (DFT) and discrete wavelet changes (DWT) and so on. In the wake of applying change, watermark is implanted in the converted coefficients of the picture such that watermark is not unmistakable. At long last, the watermarked picture is gotten by procuring opposite conversion of the coefficients [6].

Mondalet.al. proposed a new computing approach.In peculiarity based watermarking plan, watermark is produced by applying a few operations on the pixel estimation of host picture instead of taking from outer source. Late investigates on secure advanced watermarking methods have uncovered the way that the substance of the pictures could be utilized to enhance the imperceptibility and the power of a watermarking plan [7].

To enhance the security, Wang et.al [8] receive a key ward wavelet change. To exploit confinement and multi-determination property of the wavelet change, proposed wavelet tree based watermarking algorithmby Wang [9]. Tao et al. [10] set forward a discrete-wavelet converts based numerous watermarking algorithms. The watermark is implanted into LL and HH sub-bands to enhance the heartiness. Luo et al. [11] presented a number wavelets based watermarking procedure to secure the copyright of computerized information by using encryption method to improve the security.

Qiwei et al. [13] set forward a DWT based visually impaired watermarking plan by scrambling the watermark utilizing disarray arrangement.Yuan et al. [12] proposed a number wavelet based Multiple logo watermarking plan. The watermark is permuted utilizing Arnold change and is implanted by altering the coefficients of the LL and HH sub-bands. A number of the algorithms proposed meet the indistinctness prerequisite effectively yet vigor to diverse picture handling strike is the key test and the algorithms in writing tended to just a subset of assaults.

This exploration proposes a novel DWT based visually impaired watermarking plan, in which watermark is developed from the spatial space and is inserted in the high-recurrence band. As indicated by this algorithm, a DWT is performed on the host picture and values in Ll1 sub band structures the first framework. The second grid is created by discovering normal qualities from each 2x2 squares. Watermark development methodology finds the divergence values between those two frameworks and is changed over into paired structure. The resultant grid is cluttered with the assistance of Arnold Transform. The extraction methodology is carried out without utilizing unique picture and the recently created technique is vigorous against numerous basic picture assaults and test results check this. The security of the proposed strategy lies on the multifaceted method used to build watermark.

Below Table show the background analysis of research field.

SN	Name of Method	Name of the author	Publication Journal and year
1	Load Balancing in Cloud Computing using Stochastic Hill Climbing	Brototi Mondal, et. al.	Elsevier, Procedia Technology (2012)
2	Robust Digital Watermarking of Color Images under Noise Attacks	R. Reddy et. al.	IJRTE, May 2009
3	Economical Duplication Based Task Scheduling for Heterogeneous and Homogeneous Computing Systems	Agarwal, A., Kumar, P.	Advance Computing Conference, 2009
4	A Grid Task Scheduling Algorithm Based on QoS Priority Grouping	F. Dong et. al.	IEEE, 2006
5	A survey of wavelet-domain based digital image watermarking algorithm	Q.Ying, and W.Ying	Computer Engg. and applications, 2004
6	A wavelet-based watermarking algorithm for ownership verification of digital images	Y.Wang et. al.	IEEE Trans. Image Process, 2002
7	A comparison of eleven static heuristics for mapping a class of independent tasks on heterogeneous distributed systems	T.D.Braun et. al.	Journal of Parallel and Distributed Computing, 2001

DOI 10.17148/IJIREEICE.2015.3720

8	A class of authentication digital watermarks for secure multimedia communication	L.Xie et. al.	IEEE Transactions on Image Processing,

Table I: The background analysis of research field

III. DIGITAL WATERMARKING IN IMAGE AUTHENTICATION

Digital Watermarking is the method of digital multimedia content which is embedding dataso that in future the data can be identified or extracted fornumerous purposes comprisingauthentication controland copyrightprotection. The initiation of the Internet and the wide accessibility of computers and printers make digital data exchange and digital communication aneffortless task. On the other hand, making of this digital data availability to others via networks also creates possibilities for malicious parties to build salable copies of protected and patented content without copy permission of the data owner [2, 8]. To secure the multimedia content numerous technologies are used e.g. watermarking, cryptography, and steganography. Watermarking techniques are utilized for authentication and protection of multimedia data. Cryptographic techniques are utilized to modify the significance of the information or data. Steganography techniques are utilized to mask the presence of the important data.

Proposed watermarking system extracts and creates watermark content from watermarked image and so innovative image is not important. Therefore it can be called as blind watermarking [9].

The confirmationprocess consists of the following steps:

- Confirmation is done by locating the tempered regions and extraction is performed by interrelated watermark on the tempered area of watermarked image.
- Compare the two watermarks (innovative and restored). If two values equivalent, authenticity is conserved. Or else the authenticity is alleged.
- We encrypt the first watermarkthat is done in the original images by our reformed CPT algorithm. Then first encrypted watermark is correlated with the second watermark.

IV. AES WATERMARK APPROACHES

AES is a symmetric block cipher [13]. It utilizes the piece size of 128-bits and a key size of 128, 192 or 256 bits. Each one full adjusts of AES utilization four capacities: byte substitution, change, number-crunching operations, and XOR with the produced key. We utilize the security of AES-128 to scramble the first watermark picture as piece by square approach by isolating the picture into 4 hinders each of 128x 128 bits. Initial 128 bits in the first line of block# 1 are information to AES-128 module. The full square of 128 x 128 sizes is then changed over to 4 x 4 square grids of bytes. The figure comprises of N-rounds. The amount of rounds relies on upon the key length. We utilized the key length of 128 bits and hence aggregate rounds turn into 10. So we get the encoded watermark, we in aggregate 10 rounds. These rounds are taken to maintain a strategic distance from the bruit power attack.

Existing arrangement in base examination utilize the security of AES-128 [14] and install different watermarks: connected watermark images and encrypted watermark. We encrypt the first watermark by our proposedAES, and correlate the second watermark. The key watermark embedding is carried out in the first photos by an altered CPT calculation [15]. The second watermark is installed in the wavelet sub-groups. First watermark is utilized for validation purposes and second watermark is utilized for restoring the estimation of originalimage. By consolidating the restored delivery and the altered one, they restore the photo with a perfect quality.

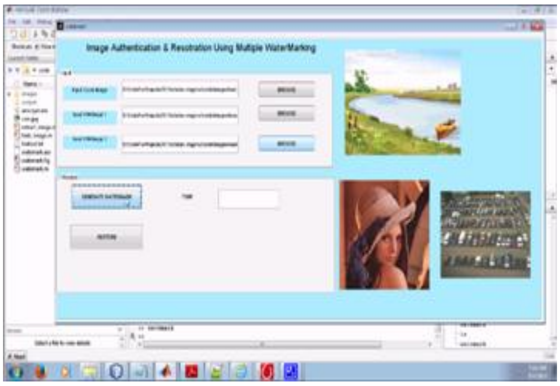
Image Authentication & Resotration Using Multiple WaterMarking

Fig.1: AES watermarking process

Fig. 1 shows the image authentication using encryption and image restoration using decryption. The software and programming platform taken is Matlab. A programming code of watermark embedded is prepared. The process of authentication and restoration is shown using three different images and embedded in the programming code. The image cryptography can be used to authenticate and secure the original images.

V. PROPOSED SOLUTION

The proposed solution is supposed to be work on following shortcomings:

- To enhance the security through image encryption.
- For finding possible path to enhance the water marking encryption technology.
- To implement the steganography technology through water marking techniques.
- Encrypting a message to improve overall security.

The existing research solution has following problems

1. AES is time consuming with more than 10 rounds. The key size is also very large.
2. Embedding in wavelet sub-bands causes noises in the original image.

So to avoid these two problems we propose following extension on the base research

1. AES with limited rounds is used.
2. Embedding in wavelet sub-bands is avoided instead unused pixel portion in all the 3 color bands is used for embedding. By this way noise is reduced.

DOI 10.17148/IJIREEICE.2015.3720

VI. FUTURE WORK

In the future enhancements we can consider the accuracy of AES with limited rounds could be used. Moreover about the embedding in wavelet sub-bands is avoided instead unused pixel portion in all the 3 color bands is used for embedding. By this way noise can be more reduced and we can get better performance.

VII. CONCLUSION

In this paper, a different watermarking plan is proposed for digital images restoration and authentication. We utilized the security of AES-128 to make anencrypted watermark and installed it in the spread picture by F -CPT algorithm for data verification. Restoration of image is accomplished by related watermark embedding in wavelet sub-groups. A few maliciousattacks are performed i.e. compression attack, cropping attack and noise attackand so on. The results of PSNR, SSIM and MSE demonstrate that the sensitivity of our framework is high and the system is exceptionally powerful.

ACKNOWLEDGEMENT

The authors convey their heartfelt thanks to **Vinith Chauhan**, HOD, SMEC Neemrana, Rajasthan, All Professors and Director Cloud Computing Group, for providing them the required facilities to complete the project successfully. This paper is used to carry out a brief review about the digital watermarking techniques in image authentication and encryption.

REFERENCES

- S.S.Sujatha, and M.Mohamed Sathik, (Sept 2010) “Feature Based Watermarking Algorithm by Adopting Arnold Transform”, Proc. of Springer International Conference on Information and Communication Technologies ICT 2010, Vol.1, pp.78-82.
- C.Rey, and J.Dugelay, (2002) “A survey of watermarking algorithm for Image authentication”, Journal on Applied Signal Processing, Vol.6, pp.613-621.
- C.I.Podilchuk, and E.J.Delp, (July 2001) “Digital watermarking: algorithms and applications” IEEE Signal Processing Magazine, pp. 33-46.
- ArvindkumarParthasarathy, and SubhashKak, (June 2007) “An Improved Method of Content Based Image Watermarking”, IEEE Transaction on broadcasting, Vol.53, no.2, pp.468 -479.
- L.Xie, S.Wang, L.Gan, L.Zhang, and Z.Shu, (2008) “A class of authentication digital watermarks for secure multimedia communication IEEE Transactions on Image Processing, Vol.10, No.11, pp.1754-1764.
- Ramana Reddy, Munaga V.N.Prasad, and D.SreenivasaRao, (May 2009) “Robust Digital Watermarking of Color Images under Noise Attacks”, International Journal of Recent Trends in Engineering, Vol.1, No. 1.
- BrototiMondal,KousikDasgupta and ParamarthaDutta, (2012) “Load Balancing in Cloud Computing using Stochastic Hill Climbing-A Soft Computing Approach”, in Proc. of *C3IT*, Elsevier, Procedia Technology 4, pp.783-789,
- T. D. Braun, H. J. Siegel, N. Beck, L. L. Boloni, M. Maheswaran, A. I. Reuther, J.P. Robertson, M. D. Theys, B. Yao, D. Hensgen, and R. F. Freund, (Jun. 2001) “A comparison of eleven static heuristics for mapping a class of independent tasks onto heterogeneous distributed computing systems,” *Journal of Parallel and Distributed Computing*, vol. 61, issue 6, pp. 810-837.
- F. Dong, J. Luo, L. Gao, and L. Ge, (2006) “A Grid Task Scheduling Algorithm Based on QoS Priority Grouping," In the Proceedings of the Fifth International Conference on Grid and Cooperative Computing (GCC), IEEE,
- Agarwal, A., Kumar, P. (2009) “Economical Duplication Based Task Scheduling for Heterogeneous and Homogeneous Computing Systems”. In: Proceedings of the Advance Computing Conference, (IACC), pp. 87-93, IEEE Computer Society
- T.D.Braun, H.J.Siegel, N.Beck, D.A.Hensgen, R.F.Freund, (2001) “A comparison of eleven static heuristics for mapping a class of independent tasks on heterogeneous distributed systems”, Journal of Parallel and Distributed Computing, pp.810- 837
- Q.Ying, and W.Ying, (2004) “A survey of wavelet-domain based digital image watermarking algorithm”, Computer Engineering and Applications, Vol.11, pp.46-49.
- Y.Wang, J.F.Doherty, and R.E.Van Dyck, (2002) “A wavelet-based watermarking algorithm for ownership verification of digital images”, IEEE Trans. Image Process, 11, pp.77-88.
- S.H.Wang, and Y.P.Lin (2002) “Wavelet Tree quantization for copyright protection for watermarking”, IEEE Trans. Image Process, pp.154-165.
- P.Tao, and A.M.Eskicioglu, (2004) “A robust multiple watermarking scheme in the discrete wavelet transform domain”, Proceedings of the SPIE, Vol.5601, pp.133-144.
- Y.Luo, L.Z.Cheng, B.Chen, and Y.Wu, (2005) “Study on digital elevation mode data watermark via integer wavelets”, Journal of software, 16(6), pp.1096-1103
- Yuan Yuan, Decai Huang, and Duanyang Liu, (2006) An Integer Wavelet Based Multiple Logo-watermarking Scheme. In IEEE, Vol.2 pp.175-179.
- H. Dobbertin, V. Rtjimen, A Sowa Ed., (2004) "Advanced encryption standard-AES," ser. Leture Notes in Computer Science/Security and Cryptography, Bonn, Germany: Springer, vol. 3373.
- Y. -C. Tseng and H. -K. Pan, (2001) "Secure and Invisible Data Hiding in 2-color Images," in Proc. of INFOCOM, pp. 887-896.
- P. -T. Huy, y' -P. Bac, N. -M. Thang, T. -D. Manh, V. -T. Duc, N. -T. Nam, (2009) "A new CPT extension for high data embedding ratio in binary images," in Proc. of KSE, International Conference on Knowledge andSystem Engineering, p. 61-66.

DOI 10.17148/IJIREEICE.2015.3720