Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 3, Issue 5; July-September, 2016, pp. 468-472

http://www.krishisanskriti.org/Publication.html

Tamper Detection and Image Recovery with Enhanced Security

Revathy S[1] and Gopu Darsan[2]

[1,2]Sree Buddha College Of Engineering
E-mail: [1]revathysreekala@gmail.com, [2]gops601@gmail.com

Abstract—*Watermark is an invisible type of signature embedded inside an image to show authenticity or proof of ownership. Watermark technique have been widely applied in various fields to protect the image against tampering. Therefore watermark algorithm have been developed to discover the tampered area and recover the lost information. This paper include source coder, channel code parity bit and check bit. Watermark technique aim to accomplish the task of tamper localization and error concealment. To easy use and analysis on computers, analog images are transformed to digital file format by digital encoding techniques. Watermarking is an information hiding technique that embeds watermark into the host image for copyright protection or integrity authentication.*
Fragile watermarking is used for both authentication and localization of tampered zone. The reference bits can protect against tampering by channel coder. The technique work by dividing an image into blocks and each block can be watermarked with a transparent watermark that sensitively depends on a secret key.

Keywords*: Image watermarking, fragile watermarking, image tampering protection, self-recovery, SPIHT, RS channel codes, prime fields.*

1. INTRODUCTION

Image processing is a process of performing some operations on an image, in order to get an enhanced image or to extract some important information from it. It is a type of processing in which input is an image and output may be image or features associated with the corresponding image. Image processing is rapidly growing technologies. It forms a research area in engineering and computer science.

Image processing basically includes the following three steps.

- Importing the image from any source
- Analyzing the image which includes data
- compression and image enhancement
- Output is the last stage where result is an altered image.

Multimedia security address the problem of digital watermarking, data encryption, authentication. The content based protection is provided in Multimedia security. The authenticity and integrity of the digital images may not be judged only by the human eyes. The digital image authentication watermarking technology, can be used to detect and locate the tampered regions. Hash of the original image is used to protect it against malicious modifications. Then hash of the output is calculated and receiver declare it as the same if the obtained value and calculated value are the same. A digital watermark is called "fragile". Fragile watermarks are mostly used for tamper detection. Modifications to an original work that clearly are noticeable. To easy use and analysis on systems, analog form images are transformed to digital file format by digital encoding techniques. Also fragile watermark can used to locate tampered zone and protect against malicious modifications. Fragile watermark are designed for binary images, JPEG compressed images, colored images.

Self recovery in watermark is divided in to two : check bit and reference bit. Check bit are used to localize the tampered block and reference bit are used to restore the original image in tampered area. Source coding and channel coding technique is used in this paper. The source coding technique is used to reduce the size of the information that is going to be being transmitted. Also redundancy is reduced. The channel coding technique is used to reduce the error during transmission of data through the channel from the source to destination and also add redundancy to data.

SPIHT method provides good image quality, high PSNR. It is optimized for progressive image transmission and provides fast encoding and decoding. It provides efficient combination with error protection. SPIHT is an image compression algorithm that aims exploit the inherent similarity across the sub bands in wavelet decomposition of an image. Wavelet transformation has become a most important and powerful tool of signal representation. Wavelet is used for image processing and compression because of low computational complexity of separable transforms. Application of wavelet transform is image compression, edge detection and noise removal.

A parity bit or check bit is a bit added to the end of a string of binary code that indicate whether the number of bits in the string with the value one is even or odd. Parity bit are used as one of the easiest error correcting code. And parity bit can be

set as even and odd. If parity bit is odd then any group of bit that arrive with an even number of ones must contain an error.

All literature papers give information about different watermarking technique permutation without source and channel coder. So the tamper detection become more complicated. SPIHT algorithm provide the image with more clarity. Digital image tampering detection aims at verifying the authenticity of digital images without any information or knowledge on the original images. Memory requirement is high and processing of robustness is less in previous techniques.

2. RELATED WORKS

Jiri Fridrich etal.[1] has proposed a method of watermarking technique for tamper detection in digital images. By comparing correlation values from different portions of the image, the technique enables us to distinguish malicious changes, such as replacing / adding features from no malicious changes resulting from common image processing operation. The watermarking method is a frequency based spread spectrum technique. To achieve a continuous dependency on the image, we propose a special bit extraction procedure that extracts bits from each block by thresholding projections onto key dependent random smooth patterns. One of the first techniques used for detection of image tampering was based on inserting check-sums into the least significant bit (LSB) of image data. Walton proposes a technique that uses a key-dependent pseudorandom walk on the image. In this paper a technique is describe that uses a robust watermark in larger blocks. To prevent unauthorized removal or intentional distortion, the watermark must depend on a secret key S (camera's ID), block number B, and on the content of the block.. cameras has its own specifics. In one possible scenario, a special tamper-proof watermarking chip inside a digital camera will watermark the image data before it is stored on camera's memory. the total memory requirements are approximately determined by the number of pixels in two blocks plus the length of the spread spectrum signal. As the pixel increases memory requirement also increased.

Meng Chen etal. [2] has proposed a set of classification-based block concealment schemes, including receiver-side classification, sender-side attachment, and sender-side embedding. The classification-based approach also helps us achieve a better tradeoff between the concealment quality and the computation complexity on the receiver side. The classification in the proposed new framework of error concealment can be done either on the receiver side or on the sender side. And determine which candidate concealment is better for corrupted block. support vector machine (SVM) classifiers, is adopted as they often exhibit good generalization performance. The linear SVM determines a linear discriminant function that gives the maximum separation margin between the two classes of training data. sender-driven perspective to provide perfect classification information to a receiver through attachment or embedding, and thus further enhance the error concealment performance. This paper take great effort in concealing corrupting the block but error concealing cannot be reduced.

Sujoy Roy and Qibin Sun [3] has proposed an image hashing approach that is both robust and sensitive to not only detect but also localize tampering using a small signature. The amount of information in the hash about the original should be as large as possible. The goal of the hashing method is to verify the authenticity of the query. Only allowably modified images are declared authentic. Tampered or distinct images are declared non-authentic. Image hashing method consists of two steps:

- Hash generation
- Verification.

For hash generation, a set of features is extracted from the image and a function maps them to a bit sequence. Lack of content information as part of the hash also leads to high false positive detection error. A clear disadvantage in using watermarking is the need for distorting the content. Search complexity and rate of noise is high.

Vu and Bede Lui [4] propose a data embedding method for image authentication based on table look-up in frequency do-main. Simple features are embedded invisibly in the marked image, which can be stored in the compressed form. Fragile watermarking is a technique to insert a signature for image authentication. The signature will be altered when the host image is manipulated. An effective authentication scheme should have some features:

- To be able to determine whether an image has been altered or not.
- To be able to locate any alteration made on the image.
- To be able to integrate authentication data with host image rather than as a separate data.
- The embedded authentication data be invisible under normal viewing conditions.
- To allowthe watermarked image be stored in lossy compression format.

A new authentication scheme by embedding a visually meaningful watermark and a set of simple features in the frequency domain of an image via table look-up. This scheme can be applied to compressed image using JPEG. The authentication data we embed in an image consists of a visually meaningful binary pattern and some content features. The scheme can detect tampering of the marked image and can locate where the tampering has occurred. Detect the tampering only in the marked area.

Ashwin Swaminathan, Min Wu and K. J. Ray Liu[5] this paper introduces a new methodology for the forensic analysis of digital camera images. The proposed method is based on the observation that many processing operations, both inside

and outside acquisition devices, leave distinct intrinsic traces on digital images, and these intrinsic fingerprints can be identified and employed to verify the integrity of digital data. The intrinsic fingerprints of the various in-camera processing operations can be estimated through a detailed imaging model and its component analysis. The presence or absence of watermarked image result in authenticity. Steganalysis methods have been proposed to identify the presence of hidden data in multimedia. Steganography is the art of secret communication where the hidden information is transmitted by embedding it on to the host multimedia. The proposed formulation is based on the observation that each in-camera and postcamera processing operation leaves some distinct intrinsic fingerprint traces on the final image. We characterize the properties of a direct camera output using a camera model, and estimate its component parameters and the intrinsic fingerprints.

3. PROPOSED SYSTEM

3.1. WATERMARKING SCHEME

The goal of this scheme is to embed a watermark into original image to protect it against tampering. It means that the watermark must be capable of both finding the tampered areas of the received image, and recovering the content of the original image in those zones. For image recovery, compress the image using a source encoding algorithm, and embed the result as watermark. However, some of compressed image information might be lost because of image tampering. compressed bit stream is channel coded using a code capable of resistance against certain level of erasure. At the receiver, the check bits locate tampered blocks.

A. Watermark Embedding

The original image I represented as 8-bit gray-scale pixel values. These eight bits are divided into four parts: The most significant bits (MSB) that will not change at the watermark embedding phase, check bits, source code bits, and channel code parity bits, denoted by nm, n_h, n_s and n_p respectively. The nm MSB bits of each pixel remain unchanged during watermark embedding and will be used for hash generation and image reconstruction. The remaining bits are used for the purpose of watermark embedding.

The permutations before and after channel coding are generated using keys $k1$ and $k2$, both derived from a secret key K, which is known to both embedding phase (transmitter end) and image reconstruction phase (receiver end), to guarantee the security of our algorithm.

B. Tampering Detection and Image Recovery

The received image which is probably tampered is decomposed into blocks of size $B \times B$. For each block, position bits are found using $k2$, derived from shared secret key. Block bits are decomposed to nm MSB bits and nw watermark LSB bits per pixel (bpp), which results in $bm = nm \times B2$ MSB bits and $bw = nw \times B2$ watermark bits.

After locating the tampered blocks, the Nc channel code bitsare collected through the whole image. The channel decoder at the receiver side is Reed-Solomon (RS) erasure decoder. Channel code bits undergo proper inverse permutation

C. Spiht algorithm for image compression

Set partitioning in hierarchical trees (SPIHT) encoding is applied as source encoder in the proposed method. SPIHT is an embedded compression algorithm, that is, one can truncate its output bit stream at the desired rate and come to a certain reconstruction of the original image. The more output rate exploited, the better quality of reconstruction is achievable. SPIHT method provide good image quality, increased rate of PSNR. It is optimized for progressive image transmission. Mainly used for encoding and decoding.

D. Channel coding

Source encoder output bits might be lost if not safeguarded because of image tampering; thus, the source encoder outcome must be protected through some channel codes. Besides, tampered blocks will be recognized using check bits. It is noteworthy that their information is available to channel decoder. Considering this source-channel code design and having error locations available, tampering can be modeled and treated as an erasure error, where the locations of error are known to decoder.

3.2. TAMPER DETECTION WITH BLOCKWISE DIVISION AND PIXEL SWAPPING

In this phase the tamper detection is performed. The accurate position of the tampered image is identified using block wise division and pixel swapping. This operation is performed before and after encoding using SPIHT and after watermark embedding. Both the operation is performed in the reconstruction phase also. This will increase the security and also identified the accurate position of the tampered image.

A. Blockwise Division

The image is performing block wise division so that each of the pixel value is calculated. Then it will more helpful in detecting the tampered position. This will increase the security of the transferring image. After all operations block wise reconstruction is performed to obtain the watermarked image.

B. Pixel swapping

It will increase the ability to detect the accurate position of the watermarked tampering. All informations regarding the image are contained in this block. This phase increase the privacy of the image. With each pixel swapping the accurate position of the tampered region is identified. After all operations then the encoded image is performing pixel swapping. After block wise

division also the pixel wise swapping is performed. This phase is helpful in detecting the tampered area accurately. The pixel wise sorting will decrease the bits discarded during error detection.

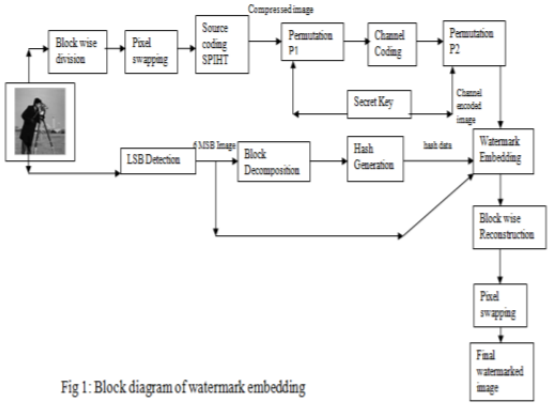

Fig 1: Block diagram of watermark embedding

Cover image is performed block wise division and pixel swapping it will increase the security then source coding is performed with SPIHT then image will compressed The permutations before and after channel coding are generated using keys k1 and k2, both derived from a secret key K, which is known to both embedding phase (transmitter end) and image reconstruction phase (receiver end), to guarantee the security of our algorithm. Then channel coding is performed which will encode the image. Then watermark embedding is performed along with in this cover image is performing LSB detection the 6 MSB of the image is block decomposed then hash generation is performed the corresponding hash data is then performing watermark embedding and block wise division and pixel swapping is done. Finally watermarked image is performed.

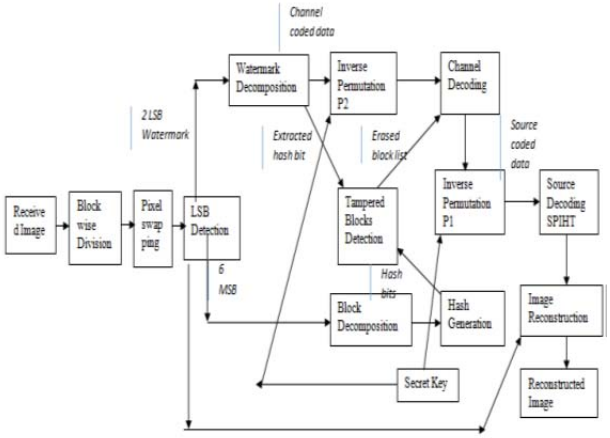

Fig 2 : The block diagram of tampering detection and image recovery

Received image is performing block division and then pixel swapping is performing LSB detection, 2 LSB watermark is then decomposed and channel code data is obtained then inverse permutation is done. For each block, position bits are found using *k*2, derived from shared secret key. The channel decoder at the receiver side is Reed-Solomon (RS) erasure decoder. The compressed image bit stream available at the output of the decoder is passed through the source decoder after undergoing proper inverse permutation. Then image is reconstructed in order to detect the position of the tampering. 6MSB of the image is block decomposed and hash generation is done. These hash bits are then doing tamper block detection and channel coding is performed. The 2 LSB watermark after watermark decomposition will extracted hash bits are passed through tamper detection and and channel coding is done in this phase. Finally source decomposition is performed and image is reconstructed and reconstructed image is obtained.

4. RESULT

Compared to the existing paper the security of the system is increased with 2 keys which performing the block wise encryption at 2 levels, which is used at the time of encoding and decoding. Also PSNR value is increased which increase the clarity of the image. By applying contrast enhancement, the features of the image become more clear than the received one. The existing system will accept tampering up to only 30%. But the proposed system will accept the rampering up to 60%. So the tampering will not be affected to our watermarked image. So the receiver will receive the water marked image without tamper and with high security

PSNR PERFORMANCE	
Existing System	Proposed System
44.84	55.76

Fig:3 PSNR performace comparison

% of Tampering acceptance	
Existing	Proposed
33%	60%

Fig4: Tampering acceptance rate comparison

5. CONCLUSION

A watermarking scheme to protect images against tampering. Watermarks are embedded once in the hiding process and it

can be blindly useful for different applications in the detection process. Hash of the original image is calculated which protect against malicious modification. Different watermarking techniques are introduced to protect against tampering.

6. ACKNOWLEDGEMENTS

First of all, we thank almighty for giving us strength and courage for taking a relevant area and to do research on that. We thank everyone, who directly or indirectly helped us for doing the thesis.

REFERENCES

[1] YanHua Liu, GuoLong Chen, and Lili Xie, "An Email Forensics Analysis Method Based on Social Network Analysis," 2013 International Conference on Cloud Computing and Big Data, 978-1-4799-2829-3/13 $26.00 © 2013 IEEE DOI 10.1109/CLOUDCOM-ASIA.2013.38

[2] Linton C. Freeman. A Set of Measures of Centrality Based on Betweenness. Sociometry, Vol. 40, No. 1 (Mar., 1977), pp. 35-41.

[3] Haibo Wang, Ning Zheng, Ming Xu, Yanhua Guo.Detecting Community Structure in Weighted Email Network[C]. proceedings of 1stInternational Symposium on Computer Network and Multimedia Technology, Wuhan, CHINA 2009.

[4] M.E.J.Newman, M.Girvan. Finding and evaluating community structure in networks. Phys.Rev.E69, 026113, 2004.

[5] Eric D. Kolaczyk, David B. Chu, Marc Barthélemy. Group betweenness and co-betweenness: Inter-related notions of coalitioncentrality. Social Networks 31 (2009).

[6] A. Swaminathan, M. Wu, and K. J. R. Liu, Digital image forensics via intrinsic fingerprints, IEEE Trans. Inf. Forensics Security.

[7] M. Wu and B. Liu, "Data hiding in binary image for authentication and annotation," IEEE Trans. Multimedia, vol. 6, no. 4, pp. 528–538,Aug. 2004.

[8] X. Zhang, S. Wang, Z. Qian, and G. Feng, Reference sharing mechanism for watermark self-embedding," IEEE Trans. Image Process.

[9] X. Zhang, Z. Qian, Y. Ren, and G. Feng, Watermarking with flexible self-recovery quality based on compressive sensing, " IEEE Trans. Inf. Forensics Security, vol. 6, no. 4, pp. 1223–1232, Dec. 2011.