A Visually Impaired Double Watermarking Using Discrete Wavelet Transform

M. Joseph selvanayagam
M. Sc (Research scholar), Dept of Computer Science, St. Xavier's College, (Autonomous), Palayamkottai, Tirunelveli, India.

Dr.S.John Peter
Associate professor, Dept of Computer Science, St. Xavier's College, (Autonomous), Palayamkottai, Tirunelveli, India.

Abstract - In this analysis a visually impaired double watermarking component for advanced color images in which undetectable dynamic watermarks are installed for copyright assurance and delicate watermarks are inserted for picture validation. With the end goal of copyright, the main watermark is inserted utilizing the discrete wavelet transform in YCbCr color space, and it very well may be extricated aimlessly without access to the host picture. Be that as it may, fragile watermarking depends on an enhanced most significant bits trade approach in RGB segments for picture validation. The genuineness and respectability of a mistrustful picture can be confirmed aimlessly without the host picture and the first watermark. The mix of dynamic and fragile watermarking makes the proposed system reasonable for ensuring profitable unique images. The exploratory outcomes showed that the proposed watermarking implement can withstand different handling attacks and a half tone based multilayer watermarking of low computational complexity also proposed. An additional data hiding strategy is also used to embed different watermarks into the watermark to be introduced to improve the security and embedding limit. At the encoder, the capable direct twofold interest procedure is used to make 256 reference tables to ensure the yield is in halftone plan. At the decoder, the estimation is considered to grow the qualifications among those delivered of the embeddings edges and reduce the required number of estimations for each point. Finally, the Bayes classifier is used to assemble the potential results of multilayer information for requesting the related focuses to expel the introduced watermarks. These decoded watermarks can be moreover secured for recuperating the additional hid layer watermarks.

Index Terms – Watermarking; secure sharing, invisible watermarking, multiple watermark, blowfish data security.

1. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Everyday tons of data are transferred through the Internet through e-mail, file sharing sites, social networking sites etc to name a few. As the number of Internet users rises, the concept of Internet security has also gain importance. The fiercely competitive nature of the computer industry forces web services to the market at a breakneck pace, leaving little or no time for audit of system security, while the tight labour market causes Internet project development to be staffed with less experienced personnel, who may have no training in security. This combination of market pressure, low unemployment, and rapid growth creates an environment rich in machines to be exploited, and malicious users to exploit those machines. Today, the world is on the anvil of being shrunk into a global net. All the systems around the world are to be used in the epoch of a nanosecond even when installed across continents and oceans. This is possible only through networks. It is in this context that networks become crucial to the viability of science and engineering research. The unprecedented growth of networking has helped in breaking all geographic barriers of the world and building the information super highway and global village.

Digital Image sharing with watermark in applications such as e-learning or remote diagnosis aid, in the propose to make the image more usable by secure using key it with a digest of its associated knowledge. The aim of such a Data hiding(DH) is for it to be used for retrieving similar images with either the same findings.

Image sharing with watermark is used in a wide variety of applications ranging from sharing secret information through image, and it also promotes applications such as remote diagnosis aid and e-learning. The basic principle of our approach is to share a image with a Data hiding (DH). The proposed DH gives a synthetic description and interpretation of the image content.

Digital Image sharing with watermark integrates metadata and/or protection data in an image by modifying its pixel gray-level values. It provides an original way to share related data, like an image and its DH. The method we use is lossless or reversible. This means that the Invisible image watermark can be suppressed from the image.

In this system, The DH associated with a single image will in fact be converted to the smallest possible binary string before its insertion in lossless medical images. The DH to be watermarked contains the total message length followed by the finding DH itself.

2. RELATED WORK

In this section, a review of different techniques and parameter estimation is made so that the image with data hide is identified and retrieve is calculated.

Kede Ma, Zhang[1]system, more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be losslessly recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. In this paper, we propose a novel method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image.

In W. Zhang, B. Chen, and N. Yu [2] method, a decompression algorithm for embedding the data is used. They proved that using this construction they can achieve the rate-distortion bound as long as the compression algorithm reaches the entropy. In this they have improved three RDH schemes that are using binary features sequence as covers. Using this system, embedding distortion can be reduced. It also improves reversible data hiding schemes for binary JPEG images. This system did not work on gray scale covers for designing recursive codes.

J. Fridrich, M. Goljan, and D. Rui's [3] system, a general framework for RDH is proposed. Extracted compressible features of cover images are firstly introduced by them. In this system, they have reserved a space to hide data by compressing the proper bit-planes having minimum redundancy. The lowest bit-planes which offer lossless compression are used if the image is not noisy. In completely noisy image some bit-planes are having strong correlations. These bit-planes are used to vacate room space to store hash. This system provides high capacity and security levels and can be used for authentication purpose of JPEG, audio file, digitized holograms etc. But this system forces noisy images to embed information in the higher bit-planes. Small images having single bit-plane cannot offer enough space to hide hash. This system has not enough capacity to embed large payload.

J. Tian has proposed a system which uses difference expansion method for embedding data. This system uses the features which are compressed by expansion i.e. the differences between two neighboring pixels. Some differences are selected for expansion by one bit i.e. the difference is multiplied by 2. Thus, LSB's of the differences are all zero and this LSB's can be used for embedding messages. The advantages of the system are: 1. Use of compression and decompression causes no loss of data. 2. This system is also applicable to audio and video data. 3. The compressed location map and changeable bit streams of different numbers are encrypted which increases the security. The disadvantages of the system are: 1. as there is division by 2 there may be some round off errors. 2. Depends largely on the smoothness of natural image that's why can't be applied to images who's capacity is zero or very low. 3. Degradation of visual quality due to bit replacements [4].

Z. Ni, Y. Shi, N. Ansari, and S. Wei have proposed a system which uses histogram shift strategy for RDH. In this system, the space is saved for embedding the data by shifting the bins of histogram of gray values. The authors make use of zero point and a peak point of given image histogram to embed messages. In this system, the embedding capacity is the number of pixels with peak point. For embedding, the whole image is searched for peak point. The advantages of the system are: 1. Simple to implement. 2. Constant PSNR of 48.0dB is obtained. 3. Distortions are quite invisible. 4. Capacity is high. The disadvantages of the system are: 1. Capacity is limited by the frequency of peak-pixel values in histogram. 2. Time consuming as image is searched several times [5].

X. L. Li, B. Yang, and T. Y. Zeng have used a hybrid algorithm which makes the combination of three techniques of PEE (i.e. Prediction-error Expansion), adaptive embedding and pixel selection. In the proposed system, depending on the threshold values the image pixels is divided into two parts. Then the pixels are selected depending on their capacity-parameter and threshold. The smooth pixels are selected from two parts. Finally, data is embedded by modifying the histograms that are derived from selected pixels. The advantages of the system are: 1. By decreasing the modifications to pixel values, the system reduces the embedding impact. 2. More sharply distributed prediction-error histogram can be obtained. 3. The visual quality of watermarked image is greatly improved [6].

L. Luo et al. have used an interpolation technique for developing their reversible image watermarking system. This system can embed a large amount of converted data into images with imperceptible modification. The interpolation errors which are residuals of this technique have greater decorrelation ability. The highly efficient reversible watermarking scheme is developed by applying additive expansion to these interpolation-errors. The advantages of the system are: 1. High image quality. 2. Greater embedding capacity. 3. Less Computational cost [7].

G. Xuan, J. Chen, J. Zhu, Y.Q. Shi, Z. Ni, and W. Su have proposed a integer wavelet transform based lossless data

hiding technique. This system hides the authentication information. For preventing gray scale overflowing during data embedding, the histogram modification or integer modulo addition techniques are used. This method uses second-generation wavelet transform IWT. The information is hided into middle bit-plane and in the high frequency sub-bands respectively. This makes the watermarked image greatly as same as the original image. Also the PSNR value is increased. The advantages of the system are: 1. High embedding capacity. 2. Security level is raised due to the use of secret key during embedding of data. The disadvantages of the system are: 1. only gray scale mapping is done. 2. Often multiple bit planes are needed to have enough space [8].

In this paper, V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi have proposed a system which gives reversible or lossless watermarking for image without using a location map. In this system data embedding depends on the prediction errors. Prediction errors based on magnitude of its local variance can be recorded using sorting technique. Using the sorted prediction errors and reduced size location map whenever needed improves the data embedding capacity by decreasing the distortion. The histogram shift significantly reduces the size of location map. The double embedding scheme in this system allows using each pixel for hiding data. The advantages of the system are: 1. Capacity can be significantly increased. 2. Double embedding scheme is used. 3. Less distortion [9].

M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran have tried to first encrypt the data and then compressing it, so that the compressor don't know the encryption key. The encrypted data is compressed using distributed source coding principles. The key will be available only to the decoder. They have shown that encrypted data can be compressed to same rate as that of original unencrypted data could have been. The perfect secrecy and original cover recovery is obtain in this system [10].

The paper is organized as follows; Section 2 shows the encryption and data hiding and this section secure encryption done by different technique and also Section 3 discusses about the results and performance analysis and finally section 4 concludes the project.

3. PORPOSED MODELLING

In this proposed to be select for Invisible image watermark for share data. When Invisible image watermark is applied to images, it allows the insertion of a data by modifying the pixel values of the image in an imperceptible manner. The embedded information is attached to the signal itself, independently of the image file format, introducing information management and protection levels as near as possible to the data. It is usually required that the Invisible image watermark and key information remains hidden from any unauthorized user.

In addition, distortions due to the Invisible image watermark should not interfere with the use of the object. For images, the image interpretation should not be altered. Among the different approaches proposed for Invisible watermark image to be retained lossless or reversible secret image with data. The reversibility property allows the removal of the negative from the image and the exact retrieval of the original image.

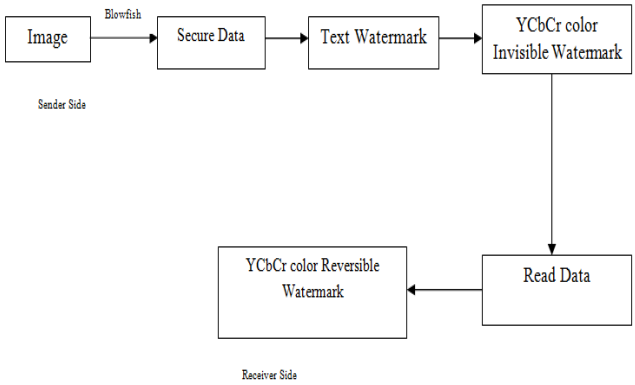

Figure 1 – Architecture diagram

Figure 1 portrays the architecture diagram of the secure image with data protection using YcbCr method and with blowfish algorithm respectively. The proposed system methodology is described as follows.

3.1 Methodology

The parameter estimation is very difficult in encryption and decryption. The proposed system helps to estimate the parameters and measure the accuracies by feature technique using encryption and decryption methods.

In the present data transfers using internet is rapidly growing because it is so easier as well as faster to transfer the data to destination. So, many individuals and business people use to transfer business documents, important information using internet. Security is an important issue while transferring the data using internet because any unauthorized individual can hack the data and make it useless or obtain information un-intended to him.

The proposed approach in this project uses a new secure image with data approach called image watermark. The application creates a hide image in which the personal data is embedded and is protected with a secure method which is highly secured.

The main intention of the project is to analyze the multiple methods and develop an application using algorithms such that it provides good security. The proposed approach

provides higher security and can protect the data from hide attacks. The image resolution doesn't change much and is negligible when embed the data into the watermark image and the image is protected with the key. So, it is not possible to damage the data by unauthorized personnel.

External Interface Requirements

User Interfaces

The system is following a consistent theme and clear structure. The occurrence of errors should be minimized through the use of checkboxes, radio buttons and scroll down in order to reduce the amount of text input from user.

Software Interfaces

Server Side

The system already has the required software to host a Matlab Simulation tool.

Client Side

An OS is capable of running modern a Matlab Common forms.

Safety Requirements

A system must be of a high integrity level and if the software is shown to be of that integrity level, then the hardware must be at least of the same integrity level. There is little point in producing 'perfect' code in some language if hardware and system software (in widest sense) are not reliable. If a computer system is to run software of a high integrity level then that system should not at the same time accommodate software of a lower integrity level.

Systems with different requirements for safety levels must be separated. Otherwise, the highest level of integrity required must be applied to all systems in the same environment.

Security Requirements

Authentication is the process of determining if a user or entity is who he/she claims to be. In this tool it is easy to confuse authentication and session management.

3.2 Proposed Blowfish Algorithm

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneider and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention. Blowfish as a general-purpose algorithm intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents or were commercial or government secrets. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in the public domain, and can be freely used by anyone.

Algorithm steps

It will convert a key of at most 448 bits into several sub key arrays totaling 4168 bytes. These keys are generated earlier to any data encryption or decryption.

The p-array consists of 18, 32-bit sub keys:

P1, P2,……., P18

Four 32-bit S-Boxes consist of 256 entries each:

S1,0, S1,1,……. S1, 255

S2,0, S2,1,…….. S2,255

S3,0, S3,1,…….. S3,255

S4,0, S4,1,.....S4,255

1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.

2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XOR ed with key bits. (For every short key, there is at least one equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)

3. Encrypt the all-zero string with the Blowfish algorithm, using the sub keys described in steps (1) and (2).

4. Replace P1 and P2 with the output of step (3).

5. Encrypt the output of step (3) using the Blowfish algorithm with the modified sub keys.

6. Replace P3 and P4 with the output of step (5).

7. Continue the process, replacing all entries of the P array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm.

In total, 521 iterations are required to generate all required sub keys. Applications can store the sub keys rather than execute this derivation process multiple times.

4. RESULTS AND DISCUSSIONS

Text Watermark Module

This module enables to create a semi-transparent, yet highly visible watermark using text and it over proprietary thumbnails and preview images to safeguard them from unauthorized use and digitally stamped with a watermark,

provided that the image is in a standard supported format, such as JPEG.

Secure image Module

Invisible image watermark is a recognizable image or pattern in this process that appears as various shades of lightness/darkness when viewed by transmitted light (or when viewed by reflected light, atop a dark background), caused by thickness variations in the project. The image watermark process has two types such as visible and invisible. In this module, to process invisible Negative images apply into the secret image.

Embedding phase

Training module takes important place in Reversible Invisible image watermark for Knowledge Digest Embedding system, because all the details regarding images are stored such as document finding attributes and so on. This module enables to embedding data regarding into Invisible image watermark secret image. The advantages are that the hidden document doesn't stand out. It can be passed in safe content like an encrypted file with password. If sender only sending something simple like secret images, that's fine.

Authentication phase

This system is mainly for share the images as well as data regarding image among group members or authenticated persons. So it's very confidential. All data as well as secret images are available. If he/she possesses the Invisible image watermark extractor with the appropriate Invisible watermark image, his/her system will extract the information otherwise data will not extract.

Security using Watermark

Image sharing is used in a wide variety of applications ranging from telediagnosis to telesurgery, and it also promotes applications such as remote diagnosis aid and e-learning. The basic principle of our approach is to share an image with a Data Holder (DH). The proposed DH gives a synthetic description and interpretation of the image content.

In the framework of an e-learning application demonstrator project, this digest will constitute the distributed knowledge and will thereafter be exploited in order to:

1) Update the user's case and knowledge bases and

2) Provide the means for similar image retrieval with either the same findings or differential diagnoses.

Watermarking integrates metadata and/or protection data in an image by modifying its pixel values. It provides an original way to share related data, like an image and its DH. The method use is lossless and reversible. This means that the watermark can be suppressed from the image.

In order to minimize the size of the whole message to be embedded, the three finding DH vectors are embedded before being process.

5. CONCLUSION

In this analysis proposed a new way to share and enhance image functionalities. While watermarking allows the sharing of information independently from the image format, the proposed knowledge digest gives a synthetic description of the image content, a digest that can be used for retrieving similar images with either the same findings or differential diagnoses.DH combined with watermarking appears to be a flexible solution to provide updates for distant user similarity rules, and case and knowledge databases. It preserves image quality and may enable other useful applications similar to the e-learning demonstrator presented.

The Future enhancement for the this process will focus on determining adaptively for any image the method parameters to ensure watermark invisibility (i.e., coefficient planes to select for embedding), optimizing the watermarking capacities of endoscopic images, in order to integrate more knowledge, i.e., the image semiology level, and managing other file image formats like the recent JPEG format.

REFERENCES

[1] Sonika C. Rathi" Medical Images Authentication Through Watermarking Preserving ROI,"in 1Department of Computer Engineering, College of Engineering Pune, Shivajinagar, Pune University, Maharashtra, India, Vol.1, No.1, August 2012.

[2] Mustafa Ulutas" Medical image security and EPR hiding using Shamir's secret sharing scheme"in Dept. of Computer Engineering, Karadeniz Technical University, 2011,pp. 341–353.

[3] Neha Solanki" ROI Based Medical Image Watermarking with Zero Distortion and Enhanced Security," in *I.J. Modern Education and Computer Science*, 2014, 10, 40-48

[4] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, and R. Collorec, "Relevance of watermarking in imaging," in *Proc. IEEE Int. Conf. ITAB,*2000, pp. 250–255.

[5] G. Coatrieux, L. Lecornu, B. Sankur, and C. Roux, "A review of image watermarking applications in healthcare," in *Proc. Int. Conf. IEEEEMBS— EMBC 2006*, Shanghai, China, Aug. 30–Sep. 3, pp. 4691–4694.

[6] Digital Imaging and Communications in Medicine (DICOM) Standard. (2007) .

[7] R. Jain, S. Antani, and R. Kasturia, "A survey on the use of pattern recognition methods for abstraction, indexing and retrieval of images and video," *Pattern Recognit.*, vol. 35, no. 4, pp. 945–965, 2003.

[8] C. Kim, "Compression of color images in gastrointestinal endoscopy: A review," *Med. Informatics*, vol. 9, pp. 1046–1050, 2006.

[9] T. Lehmann, M.G¨uld, C. Thies, B. Fischer,K. Spitzer,D.Keysers,H.Ney, M. Kohnen, H. Schubert, and B. Wein, "Content-based image retrieval in applications," *Methods Inf. Med.*, vol. 43, no. 4, pp. 354–361, 2004.

[10] A. E. Plaza, "Case-based reasoning: Foundational issues, methodological variations, and system approaches," *Artif. Intell. Commun.*, vol. 7, no. 1, pp. 39–59, 2004.

Authors

M.Joseph selvanayagam, Msc. he is doing as Mphil Research scholar in St. Xavier's College, Tirunelveli, in computer science department for the past PG degree also doing in the same college his area of interest is in Digital Image Processing.

Dr. S. John Peter, M. Sc. , M. Phil. , P. G. D. C. A. , M. Sc. , M. Phil. , Ph. D. he is working as a Associate professor in ST.Xavier's College, Tirunelveli, in computer science department for the past nineteen years. He is qualified the SLET exam and Completed Ph.D in M S University in the year 2012.And his area of interest in Data Mining.