Conditional Local Prediction Based Image Watermarking

Khushboo Pawar [1], Bhawana Pillai [2], Dr. Sadhana K Mishra [3]
M.Tech Scholar CSE LNCT(S),Bhopal (MP) [1]
Assistant Professor,Dep. Of CSE LNCT(S),Bhopal(MP) [2]
HOD CSE LNCT(S),Bhopal(MP) [3]
khushi.pawar15@gmail.com [1]

Abstract- **The enforcement and protection of rational rights of property for the digital media has grown to a significant problem in various countries in the world. There is raise in accessibility and popularity of Internet to edit, record, replicate and telecast content related to multimedia that has require a huge necessity to prevent the digital information from the illegal access, modifications and distributions. General idea of the digital watermarking is to insert the data into media cover to allow security to the data. The technique of watermarking that is fulfilling these needs known as the Reversible watermarking. In this paper, we are proposing method for watermarking. This method is using conditionals local prediction and give better results.**

Index Terms—**Image Processing, Local Prediction, Water Marking, Digital Image,**

1. Introduction

Data hiding are a group of techniques used to put a secure data in a host media (like images) with small deterioration in host and the means to extract the secure data afterwards. For example, steganography can be named [1]. Steganography is one such pro-security innovation in which secret data is embedded in a cover. But, this paper will get into reversible data hiding. Reversible data-hidings insert information bits by modifying the host signal, but enable the exact (lossless) restoration of the original host signal after extracting the embedded information. Sometimes, expressions like distortion-free, invertible, lossless or erasable watermarking are used as synonyms for reversible watermarking [2].

Watermarking technique is the process which is used to insert the proprietary information into the digital signal of multimedia allows a great solution to this issue. Few security trends should be present to prevent the records from the illegal user and information destruction. Data security has now become a requirement for each and every individual connected into the internet and uses it for any reason. It is a need that is compulsorily in every matter of the functions performed on internet.

Operations like online money transactions, transfer of sensitive information, web services, and numerous other operations need security of data. Along with these operations on the internet, data security is also essential and important in databases. Visible type of watermarks are continuously added to the digital images as a pattern of copy protection, but as

they are present so they necessarily damage the picture, eliminating information within changed pixels in a way which cannot be saved, the system which can be used for authentication purpose of the military images. Less costly software for image editing is now present which can be used to create necessarily insignificant "photo realistic" modifications to any photograph.

In a military area it is relevant to protect illegal handling of digital images and to be capable to represent the provenance and credibility. Watermarking has been used widely to prevent the copyright of the digital images. To strengthen the intellectual property right of a digital image, a trademark of the owner could be selected as a watermark and embedded into the protected image. The image that embedded the watermark is called a watermarked image. Then the watermarked image could be published, and the owner can prove the ownership of a suspected image by extracting the watermark from the image which is watermarked. It can be determine the ownership of the suspected image.

However, in some applications, especially in the medical, military, and legal domains, even the imperceptible distortion introduced in the watermarking process is unacceptable. This has led to an interest in reversible watermarking, where the embedding is done in such a way that the information content of the host is preserved. This enables the decoder to not only extract the watermark, but also perfectly reconstruct the original host signal from the watermarked work. Many of the early approaches to reversible watermarking [3], can be categorized as modulo-arithmetic-based additive spread-spectrum techniques. The use of modulo arithmetic in additive spread-spectrum techniques, which are used in traditional watermarking systems, was to ensure reversibility.

II. Data Security

Data security has become a necessity for every individual who is connected to internet and uses the internet for any purpose. It is a requirement that is a must in every aspect of the operation performed on the internet. Operations like online money transactions, transfer of sensitive information, web services, and numerous other operations need security of data. Along with these operations on the internet, data security is also essential and important in databases.

The level of security depends on the nature of information. For example, the military databases require top and high level security so that the information is not accessed by an outsider but the concerned authority because the leakage of critical information in this case could be dangerous and even life threatening. Data security is essential because they suffer from security threats that may prove harmful and disastrous if disclosed or accessed publicly. Below we will present some security threats that are suffered by the databases.

- **Privilege Abuse:** When database users are provided excessive privileges than their required functionality, then these privileges can be intentionally or unintentionally exploited.
- **Legitimate Privilege Abuse:** In this attack, the attacker with the legitimate privilege access to the database may abuse the information stored in the database for the malicious purposes.

III. Various ways of Data Security

The transfer of data in between two parties should be in done in a safe method so that to prevent any alteration. There are two kinds of threats are present while any exchange of information. The involuntary user who can attempt to wiretap this communication can either destroy this information by changing its real meaning or it can attempt to hear to message with purpose to decode it and use it for their benefits. Both of these types of attacks break the privacy and integrity of the message send. Allowing legal access and preventing illegal access is a very complicated work.

Here are explained the three main data security techniques used now: watermarking, cryptography, stegenography, fingerprinting and digital signature.

3.1 Watermarking

A watermark is an identifiable pattern or image which is affected onto the paper that gives proof of its genuineness [4]. Watermark looks as several shades of darkness lightness as when seen in light. Watermarks are mostly used as features of security to postage stamps, passports, banknotes, and other papers of security [4].

3.2 Cryptography

Crypt means “hidden or secret” and graph in means “writing”. Cryptography is a process of converting data into a format which is unreadable known as cipher text. At other side the receiver, decrypt or deciphers the message again into the plain text. It enables data’s data integrity, confidentiality, non repudiation and authentication.

3.3 Fingerprinting

Fingerprinting is a process that deals with the taking every copy of the content and create it a unique copy for the person who receives it. In this way, if the task is distributed, that to know exactly to which person initially sends the work. In other words, what the fingerprinting is normally does is it take the contents and use some types of software to transform it into a string of characters or unique number and then that string is used to match it against the other content present there.

3.4 Digital Signature

The digital signature can provide a recipient with proof of the authenticity of the object’s originator. Digital signature may be used with any type of message or information, if it is encrypted or not, basically such that the receiver may be assuring of the identity of the sender and the message reached undamaged. A digital certificate consists of the digital signature of issuing authority such that anyone may validate that the certificate is genuine.

3.5 Steganography

Steganography is a practice of hiding/concealing the message, file, image within other message, file or image. The aim is to hide the messages under other messages in such a way which does not provide the enemy to find out that a second message is available there.

Steganography is an art and the science of hidden communication. This is achieved via concealing the information into the other information, hence hiding the presence of the information communicated. From the Greek words the word steganography is originated from “stegos” meaning “cover” and “grafia” meaning “writing” [5] defining it as “covered writing”. In an image steganography, the information is concealed particularly in the images. It is separate from the cryptography in the way that in which the cryptography targeted on maintaining the secret the contents of a message, where as the steganography aimed on maintaining the presence of a message as secret.

Steganography and cryptography are two different ways to prevent the information from the unauthorized parties but none of both the technology alone is full perfect and may be
agreed. If once the existence of the hidden information is disclosed or even doubtful, then the intention of steganography is slightly broken.

Thus the power of steganography can be increased by merging it with the cryptography. The other two technologies which are nearly related to the steganography are one is watermarking and another one is fingerprinting [6]. Both of these technologies are basically related with the security of the intellectual property, hence the algorithms may have various requirements as compared to the steganography.

IV. Water Marking

Watermarking is a technique of data security. The fundamental idea of using watermarking is to embed little secret information in the digital images such that the secret information or message can never be seen. The technique of watermarking are of two types:

Visible watermark : As the name suggests, visible watermarking refers to the information visible on the image or video or picture. Visible watermarks are typically logos or text.

Invisible watermark : Refers to adding information in a video or picture or audio as digital data. It is not visible or perceivable, but it can be detected by different means.

A watermark is nothing but a semi-transparent text or image on the original image. This allows the original image viewed along with copyright protection via the image as its property of the owner. Visible watermarks are more preferred for the strong copyright protection which present in digital format. An invisible watermark is the inserted image which cannot be viewed with human eyes. Only some electronic devices or some special software helps to extract hidden data to identify the copyright owner. The process of inserting the invisible watermark in an image is known as encoding.

Watermarking Techniques are:

Spatial domain - This watermark is a process that is easy to implement and the extracting process may be done without pointing to the original image.

Frequency domain – Frequency domain will change the coefficients of an image proper transforms, like FFT, DCT, DWT.

Basically there are four types of watermarking:

Text Watermarking: Text can be added into image is called text watermarking.

Image Watermarking: Image can be added into an original image is called image watermarking [8].

Audio Watermarking: Some audio signals are added into audio clip is called audio watermarking [10].

Video Watermarking: Some video clips are added into video is called video watermarking [9].

4.1 Reversible watermarking

Reversible watermarking [7][18]is also a technique of data security which inserts the secret information in a media host without the loss of the information of host. These techniques
enable the user to recover absolutely the original image from
its watermarked image by deleting the watermark from that
image. The prediction method is used in this proposed model and the prediction errors are generated to disclose the
similarity of the adjacent pixels.

4.2 Application based on Watermarking

The following application of Digital watermarking is given.

• **Copyright protection**: It is used to identify and protect official document ownership.

• **Fingerprinting**: Fingerprints are the description of an object that tends to differentiate it from other small objects.

• Medical application: Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking.[11,12].

V. Literature Review

This paper examines the uses of local forecasting in the difference expansion reversible watermarking. For every pixel, a smallest square predictor is calculated on a square block focused on pixel and the equivalent prediction error is extended. At detection the same predictor is regained without any extra information.

The suggested local prediction is basic and it implements indifferent of the order of predictor or the context of prediction. For some specific cases of the least square predictors with same context as gradient-adjusted predictor, median edge detector or the simple rhombus neighborhood, reversible watermarking based on the local prediction are clearly outperforms the state-of-the-art model dependent on classical supplement.

The local prediction dependent reversible watermarking uses has been suggested in this paper. The model is created to provide the restoration of same predictor at the detection, and without any other information.

The local prediction dependent reversible watermarking was determined for the case of 4 different prediction situations, called as the rhombus context and any ones of the GAP, SGAP and MED predictors. The suitable sizes of block have been examined for every context. They are 8 × 8 (MED), 10 × 10 (SGAP), 12 × 12 (rhombus), 13 × 13 (GAP).

The gain obtained by further optimization of the block size according to the image is negligible. The results obtained so far show that the local prediction based schemes clearly outperform their global least square and fixed prediction based counterparts. Among the four local prediction schemes analyzed, the one based on the rhombus context provides the best results. The results have been obtained by using the local prediction with a basic difference expansion scheme with simple threshold control, histogram shifting and flag bits.

Several lossless invisible watermarking techniques have been proposed in the past. The histograms of the groups of pixels are linked to a circle. The change is selected so as to aggravate the revolution of histograms over the circle. The comparative introduction of histograms of the two groups of pixels transmits one bit of the information.

The retrieval of the embedded information and, consequently,

the reversibility process are not altered by wrapped around pixels. Furthermore, the visible quality of watermarked images never faced the issue of classic “salt-and-pepper” vestige. Definitely, the abstraction is still possible of whole inserted message after the alteration of watermarked image. This power allows transmitting the installed information from lossless to lossy surroundings [6].

VI. Proposed Work

This section deals with the new proposed watermarking method. Under this section, we will see a method which is based on local prediction.

The flowchart of the proposed system is shown in fig 1. This flowchart clearly shows that central pixel will get update only when average of all the rest pixel of the block meets one threshold condition.

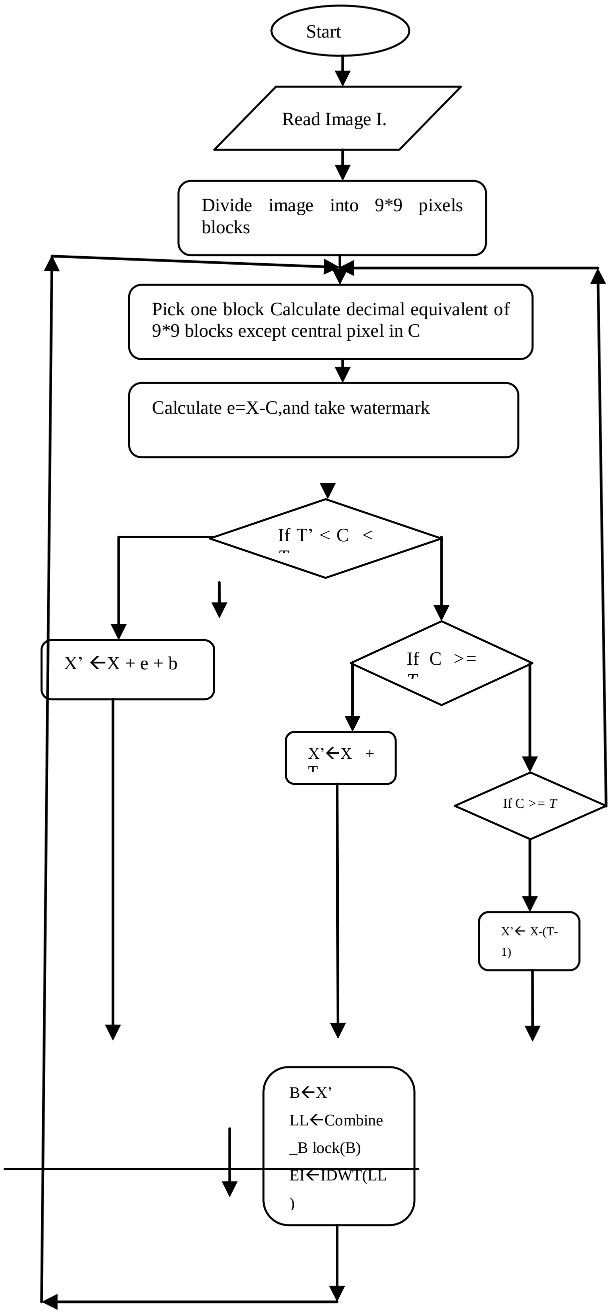

Start
Read Image I.
Divide image into 9*9 pixels blocks
Pick one block Calculate decimal equivalent of 9*9 blocks except central pixel in C
Calculate e=X-C,and take watermark
If T’ < C <
X’ ←X + e + b
If C >=
X’←X +
If C >= T
X’← X-(T-1)
B←X’
LL←Combine
_B lock(B)
EI←IDWT(LL
)

Fig 1: Flowchart of Proposed work

```
Input: Original image
Output: Embedded Image EI
LL←DWT(OI)
B←Block(LL)
$X_m$←Average(B) // $X_m$ is average of block
e←X- $X_m$ // X is original central pixel value
If T' < X  < T            // T : threshold
    X' ←X + e + b   //   b : watermark bit
ElseIf X >= T
    X'←X + T
ElseIf X<=T'
    X'← X-(T-1)
. End
```

Fig 2: Algorithm of proposed work

Algorithm of propose work is shown in fig 2. This algorithm clearly shows that watermarking will be done only when the local block level average calculation meets some particular condition.

VII. Result Analysis

Current section talks about two things. In first point, it give idea about the system, on which experiments are perform and results are evaluated. Second part idea is about the input images. Third and last part deals with the result section of the proposed work.

Part 1: System Used

1. RAM: 4 GB
2. Processor Core 2 Dual
3. Operating System: Windows 7 with 32 bits.

Part 2: Input images

This work used following two images as input images from SIPI[14].

1. Mandrila.tif
2. Lena.tif

(a)

(b)

Part 3: Parameters

This proposed work is evaluated on one parameters.

1. PSNR

PSNR: It stands for Peak Signal To Noise Ratio. It is calculated as follows. If PNSR of any image is bigger then it shows that that image is with higher quality of images

PSNR: It stands for Peak Signal to Noise Ratio. It is calculated as follows. If PNSR of any image is bigger than it shows that that image is with higher quality of images.

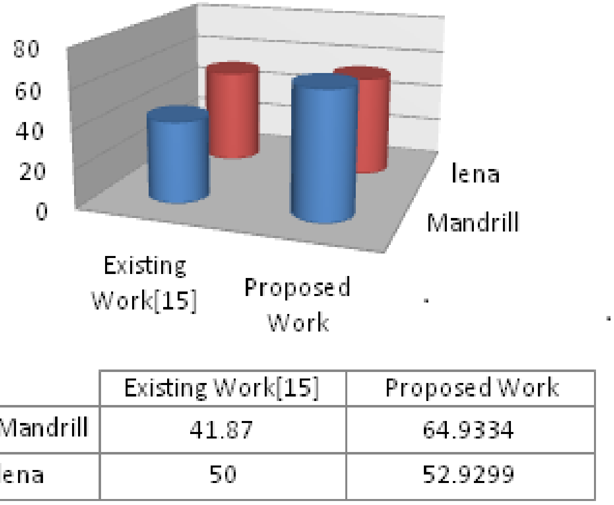
$$\text{PSNR} = 10\log_{10}\left(\frac{Max\_pixel\_value}{Mean\_Square\_error}\right)$$

Part 4: Result along with graphs

Table I and Graph 1 show the desire results.

Table I: PSNR Values of Input Image

PSNR Values of Input Image		
Images	Existing Work	Proposed Work
Mandrila	41.87	64.9334
Lena	50	52.9299



	Existing Work[15]	Proposed Work
🟦 Mandrill	41.87	64.9334
🟥 lena	50	52.9299

.

Graph 1: Comparative PSNR values of existing and proposed work

VIII. Conclusion

The There are many techniques in data hiding. Digital Watermarking is more secure and easy method of data hiding .All techniques of data hiding secure data with their methods, but watermarking is more capable because of its efficiency. In Watermarking we mark the information which is to be hiding. In this paper we have surveyed the current literatures on reversible watermarking which is a recent hot topic of research. It can have also classified reversible watermarking algorithms. Due to the space limitations we couldn't cover enough technical details but we have tried to be as clearer as possible. From the table I and II and Graph 1 and 2, very clearly say that the performance of the proposed work over existing work is much efficient.

References

1. Mehdi Hariri, Ronak Karimi, Masoud Nosrati. An introduction to steganography methods. World Applied Programming, Vol (1), No (3), August 2011. 191-195.

2. Sergio Vicente D. Pamboukian, Hae Yong Kim. Reversible data hiding and reversible authentication watermarking for binary images.

3. "Expansion Embedding Techniques for Reversible Watermarking",

Diljith M. Thodi and Jeffrey J. Rodríguez, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 16, NO. 3, MARCH 2007.

4. http://en.wikipedia.org/wiki/Watermark

5. Moerland, T., “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science,
www.liacs.nl/home/ tmoerl/privtech.pdf.

6. Anderson, R.J. & Petitcolas, F.A.P., “On the limits of steganography”, IEEE Journal ofselected Areas
in Communications, May 1998.

7. Aravind K. Mikkilineni, Osman Arslan , Pei-Ju Chiang, Roy M. Kumontoy, Jan P. Allebach, George T.-C.Chiu, Edward J. Delp, Printer Forensics using SVM Techniques , This research was supported by a grant from the National Science Foundation, under Award Number 0219893.

8. C. De Vleeschouwer, J. F. Delaigle, and B. Macq, “Circular interpretation on histogram for reversible watermarking,” in IEEE Int. Multimedia Signal Process. Workshop, France, Oct. 2001, pp. 345–350.

9. G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni, and W. Su, “Distortionless data hiding based on integer wavelet transform,” in Proc. IEEE Int. Workshop Multimedia Signal Process., St. Thomas, U.S. Virgin Islands, Dec. 2002, vol. 38, no. 25, pp. 1646–1648.

10. Aweke NegashLemma,JavierAprea,WernerOomen,and Leon van de Kerkhof, “A Temporal Domain Audio Watermarking Technique”, IEEE transaction,APRIL 2003.

11. G. Coatrieux, L. Lecornu, Members “A Review of digital image watermarking in health care”, ,Ch.
Roux, Fellow IEEE, B. Sankur, Member, IEEE.

12. Prabhishek Singh, R S Chadha, “A Survey of Digital Watermarking Techniques, Applications and
Attacks”, Proceedings of International Journal of Engineering and Innovative Technology (IJEIT),March 2013Volume 2, Issue 9.

13. Reversible Visible Watermarking With Lossless Data Embedding Based On difference Value Shift Xinpeng Zhang, Shuozhong Wang And Guorui Feng.

14. Ioan-Catalin Dragoi and Dinu Coltuc,” Local-Prediction-Based Difference Expansion Reversible Watermarking”,IEEE *transactions on image processing, vol. 23, no. 4, april 2014*