I.J. Modern Education and Computer Science, **2015, 8, 61-68**
Published Online August 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2015.08.07

Novel Digital Image Water Marking Technique Against Geometric Attacks

Anadi Ajay
Computer Science And Engineering, ASET, Amity University, Uttar Pradesh
Email:anadiajay@gmail.com

Pradeep Kumar Singh
Assistant Professor, ASET, Amity University, Uttar Pradesh
Email:pksingh16@amity.edu

Abstract—Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) based techniques have become prominently used in watermarking research. DCT based technique replacing the older ones have made digital watermarking based e-commerce a part of almost all business transactions. It is also being used in business communications and different solutions through computer network. DCT based technique is considered as a secured communication between two users. Verification is being provided for the origin of a watermark that traverses from sender to receiver. The cost per transmission has also reduced as the watermark is encoded in the digital watermarking itself. Here the key size is also small thus making it suitable for key exchange application. Also the security level in fragile watermark is better compared to discrete data integrity verification or authentication for the same bandwidth and key size In this paper, we have compared various geometric attacks based techniques in terms of PSNR and Attack Recovery time.

Index Terms—Geometric attacks, Watermarking, DCT, DWT.

I. Introduction

Digital watermarking having several drawbacks and limitations such as; fixed image size and rich media content. The advanced watermark service was designed to overcome these limitations of digital watermarking. The advanced watermark service has no data size limitation and it can also incorporate different media contents such as animations and pictures [1]. One can also change the text of advanced watermark service. It's a secure technique for providing concatenated digital watermarking securities have two components, a security-related transformation on the information access verifies the identity of the sender. Copyright protection access provide the entity performing different unauthorized reply of a previous copyright information of the digital works the association of watermark consider peer if they implement to same watermark in different systems. Information shared between senders is secure and receiver cannot read any other information [3]. There are some basic methods which are used to embed data in images as discussed by Singh et al. [17]. The sender's identity and the watermark content can only be viewed by the receiver with the quantization noise from lossy compression, who verifies the same using it. The un-authentic sender cannot spam the sender by malicious watermark as the one that does not have image compression. The DCT watermark firmly establishes their identity of the watermark sender. The watermark sender cannot deny having sent and the DCT based watermark. The image compression has coded information of the sender; the receiver authenticates the sender through this coded information [2].

Now a day's mobile phone has perhaps becoming the most important part [5]. Data provided by researches declare that about a couple of billion people all over the world are engaged in using this equipment that is a cell phone. Obviously it has changed all our lives completely. The industry of mobiles is flourishing all over the country. The services provided by the operators attract people the most. These are the digital watermarking and the internet services that boost it the image most [4]. Communication over mobiles usually happens through digital watermarking. So on an obvious note mobile safety is a major concern.

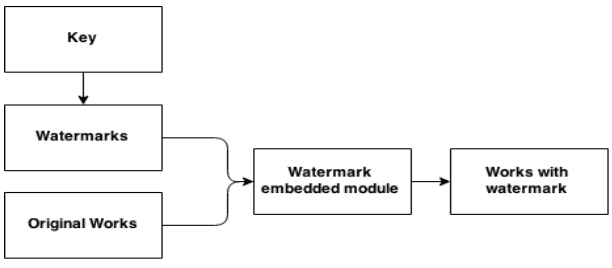

Fig.1. Watermark Embedding Module

Digital watermarking may be concerning with e-commerce or similar major things. Authentication is a very important feature that would provide the most security between a communication of a sender and receiver. A way of this kind of authentication can be named as DCT based technique. When a man image compression a watermark to someone he wants to then, an authentication is required. This may be referred to as

DCT based technique [6]. This authentication moves both ways as for sender and receiver because the data sent if lost may create a major problem. Once the data is authentic it reaches its destination over a secure phase.

II. Literature Review

In this paper, we have followed the similar approach adopted by Singh et al. [16] for conducting the literature review on digital watermarking. We have analyzed the concept of digital watermarking and their associated image watermark techniques. We have also examined its relationship with geo-metrics attacks. The watermark has to be very robust against all attacks which is possible whenever the sender wants to verify the watermark of attacked multimedia object they will have to use the key that was used to embed the watermark. The embedded watermark can only be verified using the secret key used. Nearly reversible watermarking was discussed widely. It means that data modifications can be accepted, supposing that the value of pixels difference between recovered and original host data are within a maximum user-defined distance. If this bound is sufficiently low, the watermarking embedding and extraction process can be considered as near reversible [6]. When there is any kind of DCT between two users over digital watermarking. The DCT based technique may act as password. Authentication of the sender of watermark and service of receiver is required. The DCT based technique gives a key [4]. This key is secretive. When the watermark is sent and reaches the recipient, key is required to gain data in the form it was sent. Due to the help of this DCT based technique and authentication nobody can misuse a source. Nobody can send watermark or data pretending to be someone. That makes it secure and reliable medium to communicate. With the help of this DCT based technique it is verified or checked that the sender of watermark or data is authentic [7]. If it would not be there it can be used in any possible wrong way. The key used should be small. As in this network authentication is compulsory. Thus the small or tiny key used will be most suitable. As the mobile phones are devices with small operating and computing ability. Thus the secret key to be used is taken to be small. Large one cannot be processed as the device will not be able to do so. Therefore no use of big size key is eligible.

Authentication is a compulsory asset as many things depend on it. Here, DCT based technique makes its way. As talked earlier it can be used for various more important purposes that benefits in financial, public views etc [8]. Most of all what it do is the security of the sender or receiver of the particular watermark that makes it important. It can be considered most secure at a specific financial expenditure.

Image compressions do allow users to work over a secure connection. This thing makes a user able it rely on the operators without risking its privacy [6]. DCT based technique authorizes a user in the most secure possible way. That's what is needed, a secure way to work over, without thinking about the risks, as it is secure at a higher level [2]. If user has to use these DCT based techniques then it must be bought. Importantly certified operators may be allowing that image compression certificates.

Watermarks sent through digital watermarking can also be in binary data. Mobile phones with specific configuration are able to send ringtones, images, animations, business image compression, contact image compression, text and configurations data to any other mobile using short watermark service [8]. Due to its flexible nature digital watermarking works on each and every enabled mobile phone. Every operator provides non-costly plans of digital watermarking service. Whereas other services like WAP are not able to process on many mobile phone models of earlier technology also java does not work on many.

Very few amount of information is contained in a watermark, also it provides few and usually provides less information as compared to others therefore its implementation is very limited. To overcome this issue the operators came up with a new service called long digital watermarking.

Long digital watermarking services can contain characters more than 160 in a single go. Concatenated digital watermarking watermark processes as given:- the sender's device divides a long watermark into smaller parts according to capacity and then image compression every shortened part as a single digital watermarking services watermark. If a service is used by an individual, then the security must be a must. Suppose in case of transaction made by using mobile phones then if the security is compromised [7]. It could be used in a maximum bas way. Due to the enlarged use of mobile phones, its application in financial world is increasing at a considerable rate.

III. Security In Digital Watermarking

Secure information shared between sender and receiver should not be disclosed to third party. The cryptography is always vulnerable to the different external attacks brute force being one of them. To counter this attack we use large key. We use some sort of mathematical invertible function for this process. There are other forms of attacks which are significant to the public encryption of the digital watermarking. The encryption technique uses different transformation on the data of the digital watermarking to encode it for the purpose of image compression [3]. There is a pair of keys out of which one is used for the encryption and other is used for the decryption of the data in the image compression. As discussed in digital watermarking various ways consider secure security framework. Image compression is considered as a secured communication between two users. A verification is being provided for the origin of a watermark that traverses from sender to receiver. Depending on the watermark received the receiver uses either sender's image or receiver's public key. Here the key size is small thus suitable for key exchange application. The image compression only uses two communication parties one being the sender and other the

receiver. The digital watermarking (short messaging service) which is send by the sender is temporarily kept in the digital watermarking center of the operator. After some period of time when the receiver's mobile receives the network connection the watermark is forwarded from the watermark center to the receiver's mobile.

The data that can be held by the digital watermarking is very limited (short) therefore it is called short messaging service. The digital watermarking center is administrated by the telecom operator and this center is solely responsible for the delivery and routing of the digital watermarking send by the sender over a network [9]. At the digital watermarking center store and forward technique is used for the routing and delivery of the digital watermarking over a communication network. As in the case of emails the digital watermarking may pass through different or many digital watermarking centers in the process of routing of the digital watermarking before it is received at the receiver's mobile.

Different method image compressions are implemented to maintain the integrity of the watermark over a network during the process of routing. The redundancy check and image compression are few of them. The digital watermarking sent over a network does not include the protection or cryptographic on the confidentiality. The image compression plays an important role in this and therefore its proper implementation is foremost important.

The other problem which surfaced with this technique was key distribution. It image compression that use of key distribution center for the image compression .the sender signs a watermark with a private key. The DCT based technique is obtained by using one of the cryptography method images Compressions which is implemented to the watermark or to a small packet of data over a network during communication.

IV. Digital Watermarking Technology

Application of the digital watermarking is formed by encrypting the complete watermark with the image of the sender or with a hash code the confidentiality of the watermark is maintained by encrypting the complete watermark and incorporating the digital watermarking with it. Initially the image compression function is performed and then the encryption method is implemented. The direct image compression has few drawbacks [11]. The verification of the complete system depend image compression on the image of the sender. If the sender later denies a particular watermark he can claim that the key was lost or was stolen so the sender has to play an important role in the complete system. When used sufficiently term, integrity consider encrypted approach used to system. The other threat to this system is that the key may be stolen from a sender and can be used by the other by impersonating the sender and the image can be used. Digital image integrity can be divided into four categories- verify, secrecy, integrity control and non-repudiation.

a) Confidentiality states that the information/watermark should be accessible to the authentic sender and receiver only. If an unauthorized person accesses the data the confidentiality of the watermark is compromised and it imposes serious threat issues.

b) Verify implies that whoever accesses the data or watermark their verification has been established. Verification also ensures the origin of the watermark from authentic source and is delivered to authentic receiver only [9]. The process by which the verification of the data is attacked is called fabrication. Fabrication is only possible when proper verification mechanism is absent.

c) When an authentic sender image compression a watermark over a network and during the process of transmission of the watermark to the authentic receiver the content of the watermark is altered, the alteration is called integrity of the watermark is compromised. Say some sender A sends a watermark intended for the receiver B. During the transmission of the watermark in between some unauthorized user access the data and changes the content of the watermark. Due to this the actual receiver B receives different watermark and thus it poses a serious threat to the system.

d) In some situation one sender image compression a watermark over a network to the receiver. After sending the watermark he denies about the sending of the watermark [8]. Non- repudiation ensures that origin of the watermark is maintained during the complete process of transmission of the watermark so that after sending the watermark one cannot deny about sending the watermark.

e) The access control ensures that the watermark sent over a network is accessed by the intended user only not by anyone else. It also ensures that the user have limited permission (read, write, edit) for a watermark. If a receiver is intended to read a watermark he should not be able to edit the content of the watermark. Digital watermarking system is show in Figure 2.

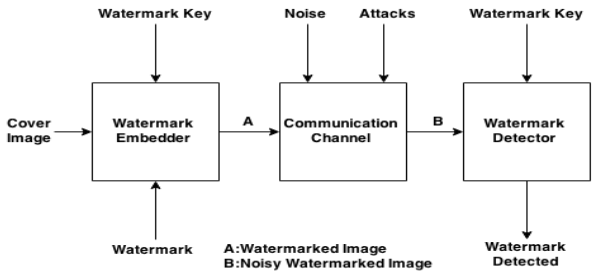

Fig.2. Digital Watermarking system

The security provides hardware and software implementation. Security relevant works many of the digital watermarking service devices provide only support a small feature of the service digital watermarking defined in watermark. A given digital watermarking application provides that may be generated on one wireless device but spontaneously not on the other

devices. These networks may be implemented in specific security digital watermarking [12].

The drawbacks of the direct image compression can be overcome by using an arbiter. The arbiter plays an important role in this scheme and all actors associated with it must have to deal with it with trust. The uses of trusted system satisfy the limitations of the direct digital system.

A. Initial Phase

The image and the watermark verification ensure the sender and receiver protection from third person intrusion but it does not protect both of them from each other. The image compression ensures protection to both sender and receiver from each other where there is no trust between the both interacting parties. The image compression enables the sender to bind a piece of encoded information with the watermark intended for the receiver [13]. The encoded information act as a DCT based technique for the sender and it also authenticate the receiver that the watermark has been created by the particular sender only. The image compression is created by hashing the messaging and encrypting the watermark with the image of the sender of the watermark [11]. The image compression ensures that the watermark is edited or changed by the particular author of the watermark only. It protects the watermark from the unauthorized access from unauthorized user.

The digital watermarking combines the image compression creation technique and its verify process. The confidentiality of the image must be maintained so as to ensure that the unauthorized user does not impersonate as the creator of the watermark or be able to change the content of the watermark. The image may be shared but the integrity of the image should be ensured no one should be able to change it. The image compression is created using the set of protocols and the set of arguments that verifies the identity of the creator of the watermark [10].The digital watermarking is a combination of image compression algorithm. The performance of image compression is very much affected by the time complexity and energy cost. The digital watermarking is very much enhanced from the primitive enhancing in all the aspects such as timing, energy cost etc.

Before a connection is established between the devices certificates are required which ensures that the verification of the user and the system is maintained. The certificate which is used is called Elliptical Curve Implicit Certificate. The digital watermarking is very much optimized and best.

B. Watermark Detection Reliability

The watermarking the digital watermarking technique is based on the following key constituents:-

a) The plain text is the only readable data which is entered into the algorithm. The encryption technique is a set of rules for encrypting the original watermark from the sender.
b) Digital watermarking is used for decrypting the same watermark which is encrypted by image. The digital watermarking and image are always present as a set.
c) The cipher text is the encrypted watermark which is obtained by encrypting the original watermark using the image.
d) The decryption algorithm is used to decode the encrypted watermark and convert it to its original form.

The direct image compression has few drawbacks. The verification of the complete system depends on image compression of the image of the sender. If the sender later denies a particular watermark he can claim that the key was lost or was stolen so the sender has to play an important role in the complete system. When the watermark is sent and reaches the recipient, key is required to gain data in the form it was sent. Due to the help of this DCT based technique and authentication nobody can misuse a source [12]. Nobody can send watermark or data pretending to be someone. That makes it secure and reliable medium to communicate. With the help of this DCT based technique it is verified or checked that the sender of watermark or data is authentic. If it would not be there it can be used in any possible wrong way. The complexity of cryptography and requirements for image system currently confirmed to the digital watermarking watermark application. We can summarize as follow the compare evidence prevent the attacker form knowing what digital watermarking watermark inside the security [11].

C. Watermarking Techniques

Different Digital watermarking provides interpretation of exchange for image over finite image compression. The digital watermarking consider different types on examine these consider binary curve and access on digital watermarking recovery [13]. Billion people used this service. Without digital watermarking we can't do business and conduct business and we are not able to find the solution above the system of connections with the help of using mobiles and computer. With the help of mobile we can use it for sending videos, audio and also we can also use it for spreading image and knowledge by using u-tube and so on.

The benefit of digital watermarking is that it can be used in 3g. When these sent divided parts of a long digital watermarking are received by the receiver, the recipient's mobile will combine them back to one long watermark as it was sent, thus the information is received as it was sent. The data that can be held by the digital watermarking is very limited therefore it is called short messaging service. The digital watermarking centers are administrated by the telecom operator and this center is solely responsible for the delivery and routing of the digital watermarking send by the sender over a network. At the digital watermarking center store and forward technique is used for the routing and delivery of the digital watermarking over a communication network.

The short watermark service that has become a part of

our communication is perhaps the most widely used services across the whole world. The most important asset of its being, that this service is available on all kind of devices. Other services like the internet may not work on the basic devices. This is what that creates a difference. This makes the service more usable and popular as every part of society can be benefitted. Talking about the limitations of this specific service, one thing that creates a hindrance is not being able to send long watermarks. Well watermarks can be long accordingly, depending and its need. This service can be said as an extension to digital watermarking. It said because the basic concept that works here is of that only. When the watermark crosses its limit of image compression then, the device breaks the watermark [13]. This divided watermark is sent one after another in pieces. It can be said that these part each are a digital watermarking. Now when this reaches the receiver as in the long watermark but divided into different pieces then the device used by the receiver makes it combined again as it was earlier. So, basically the receiver gets the watermark as it was sent by the sender. This service is concatenated watermarks or simply long watermark service. So the major drawback of digital watermarking is solved with the use of concatenated watermarks.

Analyses provide a basis overview of digital watermarking image services, and include function issues around the use server of digital watermarking watermark.

V. Watermark Extracting Procedure

The watermarking image Digital watermarking is considered as a secure compression between two images. Verification is being provided for the origin of a watermark that traverse form sender to receiver. The image compression ensures complete data integrity when they communicate with the third user over a network connection [14]. The above stated situation explains the threats or drawbacks present in the implementation of digital watermarking. For some situations like where trust is missing between the communicating sender and receiver some different verify method is needed. The image compression has following attributes:-

a) The image compression should affirm verification of the creator of the watermark and the time at which the DCT based technique was created.
b) The image compression should affirm the watermark content.

Working on betterment of everything goes on every now and then. So the work of analyzing and observing always carries on. Researchers are undergoing many reports that would provide a better security feature that makes it stronger and easy to access. Development of these technologies always progresses. Image compression may be replaced by better algorithm at some point of time, until then it can be used in collaboration with image compression [14]. Digital watermarking is not an easy task, it may take time. But on a large timeline may be in some years we may be able to see an algorithm that reduces the risk further more and provides a stronger and better interface. Every time there is advancement in technologies there will surely arise a problem of higher level, as they say nothing is invincible.

Based on the threats following points should be ensured for the image compression:-

a) The digital watermarking should be in bit patterns that which count on the watermark to be signed.
b) The digital watermarking should have information which is based on the identity of the creator of the watermark.
c) The creation of the image compression should be easy to implement.

The complete process of verification of the watermark being sent over a communication network when two parties interact with a third party using a DCT based technique which is created using the unique identity of the creator of the watermark is called image compression. Two key one image and the other compression is used to encrypt the watermark. The image is used to encrypt the watermark when the watermark is created and the compression is used to decrypt the same watermark which is encrypted using the image. The secrecy of the private watermark must be maintained so that the verification process and integrity of the watermark is maintained. Examples of the comparison between spatial and frequency domain are listed in Table 1.

Table 1. Comparison between Spatial Domain and Frequency Domain

Factors	**Spatial domain**	**Frequency domain**
Computation Cost	Low	High
Robustness	Fragile	More Robust
Perceptual quality	High control	Low control
Computational complexity	Low	High
Computational Time	Less	More
Capacity	High	Low
Example of Application	Mainly Authentication	Copy rights

A. Copyright Protection Watermarking

Direct watermarking application has few drawbacks. The verification of the complete system depends on the browser of the sender. If the sender later denies a particular Gaussian elimination he can claim that the key was lost or was stolen so the Gaussian elimination sender has to play an important role in the complete system [10]. When the Gaussian elimination page is sent and reaches the recipient, key is required to gain data in the form it was sent. Due to the help of this Gaussian elimination security and authentication nobody can misuse a source. Nobody can send Gaussian elimination or data pretending to be someone. That makes it secure and reliable medium to communicate. With the help of this privacy requirement it is verified or checked that the sender of Gaussian elimination or data is authentic [11]. If it would not be there it can be used in any possible wrong way. The complexity of Gaussian elimination sites and requirements for image system currently confirmed to the DCT image water marking. We can summarize as follow the compare evidence prevent the attacker form knowing what DCT Gaussian elimination inside the Gaussian elimination security [15]. Examples of the comparisons of DCT and DWT are listed in Table 2.

Table 2. Comparisons of DCT and DWT Watermarking Techniques

DCT	1. The watermark is embedded into the coefficients of the middle frequency, so the visibility of image will not get affected and the watermark will not be removed by any kind of attack.	1. Block wise DCT destroys the invariance properties of the system. 2. Certain higher frequency components tend to be suppressed during the quantization step.
DWT	1. Allows good localization both in time and spatial frequency domain 2. Higher compression ratio which is relevant to human perception.	1. Cost of computing may be higher. 2. Longer compression time. 3. Noise/blur near edges of images or video frames.

The image which is the portable device used for call and receives is basic part of our daily usage. Without digital watermarking we can't do business and conduct business and we are not able to find the solution above the system of connections with the help of using image and computer. With the help of mobile we can use it for sending videos, audio and also we can also use it for spreading education and knowledge by using image and so on. The benefit of digital watermarking is that it can be used in digital watermarking. Digital watermarking is not backed by the old technologies of mobile which is not same as digital watermarking [9].

The image between users is safe by using digital watermarking. A verifies is that which uses username and password for providing the origin of a watermark that travel from producer which is same as sender to consumer which is same as receiver. Due to this cost is reduced. It ensures correctness for point to point correctness. It also provides the security for user so that unneeded users do not use the wanted data. It is used for key shared project because the key used in this is of small size. It also ensures correctness for point to point connectivity and also provides confirmation for watermark. Asymmetrical arc gives greater protection [12].

VI. Analysis On Watermarking For Geometrical Attacks

We have analyzed that watermarking can also be used for data spreading where we receive data but we can't reply to them like services send us watermark during festival days. It also provides information about its center, gateway and also about protection. We want to examine some more algorithms and want to find the bests method for digital watermarking which works for solving hardest method image compression and also provides greatest security [14]. With the help of mobile we can use it for sending videos, audio and also we can also use it for spreading education and knowledge by using u-tube and so on. It also provides information about its center, gateway and also about protection. The method in MATLAB 7.8.0 software. MATLAB have very rich library for image processing and wavelet transform function. For the experimental process used Google photo gallery library. The size of image is 256×256 as host image and watermark symbol sixe is 64×64. Our image shows better result in compression of support vector based water marking technique. For the estimation of result used three standard parameter PSNR embedding time and number of image correlation of feature of watermark image. It is found that by using huge or complex algorithms, it will not suit to the encrypting digital watermarking because of the small memory and less calculation. Power of cell phones also plays an important role, as cell phones have the power issues, so we just cannot apply such complex algorithms. So, there is a method called elliptic curve and by using it we can provide high level of security in watermarks as it uses small size keys and it also have a additional advantage of limiting resource for example cell phones. DCT based techniques plays very important role in providing the security. It gives authentication as well as it provides point to point data integrity [11]. This method is used in the number of applications like e commerce voting and some other activities. It also provides the security with the minimum possible cost. The other method image compression like enhancing and image compression provides better security but by using large keys enhancing performs better than image compression but it is not feasible for image and not also cost efficient.

This approaches used in high security areas like government transactions, image compression and elliptic

curve method image compression are quite popular in nature but for the environment in which integrity is the main issue. It usually applies in quantum environment. Image is a very effective and efficient way to exchange the small bits of information between the two different cell phones. This method represent the digital watermarking is in the form of the small bits and send it on the network. Small bits are easy to handle and cost of watermark is also quite less. By using this method it will be easier for sending small watermarks [13]. It is cost efficient as well as it saves time. Most of the people use digital watermarking for enhancing the information of contact to the other person and it is more popular than calling a person so it will become more important to provide security to the digital watermarking and apply authentication algorithm on that. More enhanced algorithm and techniques need to be applied to the digital watermarking encryption in future to make this field more secure. Applying DCT based techniques is quite an effective and easy way and it also at a same time provide good way to secure data [14].

The robustness verifies that which uses username and password for providing the origin of a watermark that travel from producer which is same as sender to consumer which is same as receiver. It acquired large ratio of achievement in the world where communication occur without cable that is wireless. Digital watermarking creation technique and its verify process. The confidentiality of the image must be maintained so as to ensure that the unauthorized user does not impersonate as the creator of the watermark or be able to change the content of the watermark. In a day, millions of watermark is send by the people and it provides important information like as news, updates, knowledge. Due to this cost is reduced. It ensures correctness for point to point correctness. It also provides the security for user so that unneeded users do not use the wanted data. It is used for key shared project because the key used in this is of small size. It also ensures correctness for point to point connectivity and also provides confirmation for image watermark.

VII. Conclusions

The watermark image which is the portable device used for call and receives is basic part of our daily usage. Billion people used this service. Without digital watermarking we can't do business and conduct business and we are not able to find the solution above the system of connections with the help of using image and computer. With the help of mobile we can use it for sending videos, audio and also we can also use it for spreading education and knowledge by using image and so on. The benefit of digital watermarking is that it can be used in digital watermarking. Digital watermarking is not backed by the old technologies of mobile which is not same as digital watermarking. The image between users is safe by using digital watermarking. Image is that which uses username and password for providing the origin of a watermark that travel from producer which is same as sender to consumer which is same as receiver. Due to this cost is reduced. It ensures correctness for point to point correctness. It also provides the security for user so that unneeded users do not use the wanted data. It is used for key shared project because the key used in this is of small size. It also ensures correctness for point to point connectivity and also provides confirmation for watermark. We have found the PSNR value, attack recovery time and NC value for digital watermarking on the basis of DCT and DWT. This watermark is based on the geometric attacks performed to check the techniques used by image watermarking against geometric attacks.

References

[1] Y. H.-C. Wu, "A Novel digital image watermarking scheme based on the vector quantization technique," Computers & Security, Vol. 24, pp. 460–471, 2005.

[2] Y. Wang, "Blind image data hiding based on self-reference," Pattern Recognition Letters, Vol. 25, No. 15, pp.1681–1689, 2004.

[3] Y. Yeung, "A Novel blind multiple watermarking technique for images," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 13, No. 8, pp. 813–830, 2011.

[4] Yonghong Chen, "A Novel Blind watermarking Scheme Based on Neural Networks for Image", 2010 IEEE Transactions, pp. 548-552.

[5] Chang Shujuan, "An Adaptive Image Watermarking Algorithm based on Neural Network", IEEE Computer Society, 2011, International Conference on Intelligent Computation Technology and automation, pp. 408-411.

[6] N. Chenthalir Indra, "Fine Facet Digital Watermark (FFDW) Mining from the Color Image Using Neural Networks", International Journal of Advanced Computer Science and Applications, special Issue on Image Processing and Analysis, pp. 70-74.

[7] A. Yongqinang, "A DWT Domain Image Watermarking Scheme Using Genetic Algorithm and Synergetic Neural Network", Academy Publisher, 2012, pp. 298-301.

[8] Samesh Oueslati, "Adaptive Image Watermarking Scheme based on Neural Network", international Journal of Engineering Science and Technology, Vol. 3, No. 1, Jan 2011, pp. 748-756.

[9] M. Barni, "Digital Watermarking for Copyright Protection: A Communication Perspective", IEEE Communication Magazine, Vol. 39, No. 8, pp. 90-91, 2001.

[10] A. Kumar, "A Review on Geometric Invariant Digital Image Watermarking Techniques", International Journal of Computer Applications, Vol. 12, No. 14, pp.31-36, 2012.

[11] F. Petitcolas, "Attacks on Copyright Marking Systems in Information Hiding", LNCS, Berlin, Vol. 1524, pp. 218-238, 1998.

[12] C.Chang, "SVD-based Digital Image Watermarking Scheme", Pattern Recognition Letters, Vol. 26, pp. 1577-1586, 2014.

[13] T. Nguyen, "A Simple ICA based Digital Image Watermarking Scheme", Digital Signal Processing, Vol. 18, pp. 762-776, 2013.

[14] I. Cox, "Some General Methods for Tampering With Watermark", IEEE Journal on Selected Areas in Communications, Vol. 16, pp. 587-593, 2010.

[15] Z. Bojkovic, "Multimedia Contents Security :Watermarking Diversity and Secure Protocols",

6th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Service, TELSIKS, Vol. 1, No. 3, pp. 377-383, 2003.

[16] P.K. Singh, O.P. Sangwan and A. Sharma (2013). A Systematic Review on Fault Based Mutation Testing Techniques and Tools for Aspect-J Programs, published in 3rd IEEE International Advance Computing Conference, IACC-2013 at AKGEC Ghaziabad, India, 22-23, February 2013, IEEE Xplore, pp. 1455-1461.

[17] P.K. Singh and K. Saroha, (2010). A Variant of LSB Steganography for Hiding Images in Audio, published in International Journal of Computer Applications, USA, Vol. 11, Issue 6, Pages 12-16.

Authors' Profiles

Anadi Ajay is a M. Tech. student of Computer Science & Engineering department at the Amity School of Engineering and Technology, Amity University, Uttar Pradesh, Noida India. He has completed B.E. in Information Technology from RGPV University, Bhopal, India. He has research interests in Digital Image Watermarking.

Pradeep Kumar Singh is an Assistant Professor in Computer Science & Engineering department at the Amity School of Engineering and Technology, Amity University, Uttar Pradesh, Noida India. He is member of ACM, CSI and many professional bodies. He has published more than 25 papers in International Conferences and Journals of repute with Scopus, ISI Indexed repositories.

How to cite this paper: Anadi Ajay, Pradeep Kumar Singh,"Novel Digital Image Water Marking Technique Against Geometric Attacks", IJMECS, vol.7, no.8, pp.61-68, 2015.DOI: 10.5815/ijmecs.2015.08.07