International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

DISCUSSION ABOUT THE CHARACTERISTICS, TYPES, AND APPLICATION IN TERMS OF WATERMARKING

CANDIDATE NAME-NAME- DEV KUMAR GOLE
DESIGNATION- RESEARCH SCHOLAR SUNRISE UNIVERSITY ALWAR
GUIDE NAME- DR.SUNIL DAMODAR RATHOD
DESIGNATION- Assistant professor SUNRISE UNIVERSITY ALWAR

ABSTRACT
Now days so many people have regular web access and use application like email, instant messaging, and social networking, online messaging, etc. To speed up this communication, there is need of digital media like Text, Image, Audio, and Video. These media transfers over an open public network, hence there is need to protect these data. From all these digital media, Digital image is most widely transferring files over the network than any other but in most unsecure manner. So that some system must be there making them secure from threats and different kind of attacks over the network. This research work develops an image watermarking technique with hybridization of spatial and frequency domain image watermarking techniques. Here, this work is divided in two parts: watermark embedding and watermark extracting. There is hybridization of three techniques: DWT, DCT and SVD used in both parts watermark embedding and extracting. DWT (Discrete Wavelet Transform) is wavelet based transform that gives information about image in both frequency and spatial domain. DWT gives higher robustness, but the quality of the image is degrading. DCT (Discrete Cosine Transform) is orthogonal transform that transform image spatial domain to frequency domain. DCT gives better quality of image with less processing power. In this work an improved SVD-ARNOLD-LSVR algorithm; the host image of size 512 x 512 is embedded with the watermarks of size 128 x 128. To prove the reliability of the algorithm several images are analysed and the samples alone taken into account.

Keywords: - Watermark, Data, Digital, Network, Computer.

I. INTRODUCTION

For the past few years, there has been extraordinary progress in computer networks and predominantly, the World Wide Web. This observable fact, together with the exponential increase of computer performance, has made ease the distribution of multimedia data such as images, audio, video, and more. However, the publishers, artists, and photographers are reluctant to share pictures over the Internet due to the lack of security, i.e., the images can be easily duplicated and distributed without the proprietor's permission. Digital Watermark based cyber security systems have been providing an efficient way to deal with this tiring issue. This digital signature can forbid copyright infringement and may help to find out the authenticity and ownership of an image. Over the past several years, there has been a drastic increase in copying and sharing patented multimedia data such as video, audio, images, and software over the internet. Due to the emergence of peer-to-peer file sharing systems, this problem has become more critical. These systems let each PC to act as a file server for the networks and to share illicit multimedia data. Thus, there is a strong need to protect

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

the rights of the authors. There are many possible solutions, and one such solution is cryptography, which carries out encryption and authentication of digital data, thus allowing the point to point information exchange and transactions. Hence, once the receiver validates and decrypts the data, the product can be stripped of any content identification, proof-of ownership or other descriptive information, and any further copying and redistribution can leave the rights holders powerless and royalty-less.

Such redistributions could have disastrous implications for the entertainment industry, whose content has a long lifetime. To conquer those problems faced in cryptography, a technology called Digital Watermark based cyber security system is developed that allows some secure auxiliary information to be embedded into the original content via any channel, format or medium. Digital Watermark based cyber security system can be applied to an image, audio or a video signal. A significant development in this technology has also brought some problems other than its advantages. The great facility in copying a digital content hurriedly, flawlessly, and without limitations on the number of copies gives rise to copyright protection problem. Digital Watermark based cyber security system is conventional to prove the ownership of digital data. In watermark, a secret indiscernible signal is embedded in the original data in such a way that it remains present as long as the perceptible quality of the content is at a satisfactory level. In the case of multiple ownership claims, the proprietor of the original data proves his/her possession by extracting the watermark from the watermarked content. Here, initially, the secret signature (watermark) is implanted into the cover image by using a secret key at the cover (C). Only the proprietor of the data knows the key, and so, it is impossible to take out the message from the image without the knowledge of the key. After that, the watermarked image passes through the transmission channel. While transmitting, however, some possible attacks happen in the communication channel, namely, lossy compression, geometric distortions, any signal processing operation, digital-analog & analog-digital conversion and so on.

II. DIGITAL IMAGE WATERMARKING

Digital Watermark based cyber security system has drawn the attention of numerous researchers in the epoch between early to mid-1990s. From this period onwards, the amount of publications per year has raised quickly to several tens. It originated from simple techniques, providing the basic principles to advanced communication theory results oriented algorithms and applying them to the watermarking problem. The essential elements in an image watermarking algorithm are the cover image, watermark structure, embedding algorithm, and extraction or detection algorithm. Digital Watermark based cyber security system provides the way or technology by which the owner can conceal his/her information, for, e.g., a number or text, in digital media, such as images, video or audio.

The embedding is done by changing the content of the digital data, which means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For, e.g., the changes of the pixel values of images have

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

to be indiscernible. Depending on the application, the watermark must be either robust or fragile. The term "solid" represents the ability of the watermark to resist the manipulations of the media, such as lossy compression (where compressing data and then compressing it retrieves data that may well be dissimilar from the original, but is close enough to be useful in some way), scaling, and cropping, just to enumerate some. In some situations, the watermark may need to be "fragile" that is, the watermark should not oppose tampering, or would resist only up to a certain fixed level.

A Digital Watermark based cyber security system is a bit of information inserted in the digital media and concealed in the digital content in such a way that it is tied up with the data. In any watermarking approach, the trade-off always exists between the potency of the watermarking algorithm to signal processing attacks and the transparency of the watermark. It is assured that when the strength of the watermark is increased, the probability of full retrieval of the watermark is also increased. However, by increasing the watermark energy, the noise in the signal gets greater and thus makes the watermark perceptible. Digital Watermark based cyber security system is a competent technology, which deals with the security problems that are unsolvable by cryptography. Rooted in steganography, which is the art and science of hiding the very existence of the secret message, Digital Watermark based cyber security system provides proof and tracking capability to illegal copying and sharing of multimedia information. Three kinds of protections are required in a secure multimedia transaction: secure communication, use control and proof & tracking tool. They are correlative to defend the interests of all parties involved in a media commerce transaction.

III. WATERMARK CHARACTERISTICS, TYPES, AND APPLICATION

Many essential characteristics watermark exhibit. Some of the important ones are described below.

1. Fragility

Fragility is the most significant requirement in watermarking system, and it refers to the perceptual similarity between the original image before watermarking process and the watermarked image. In other words, the watermarked image should look similar to the original image, and the watermark must be invisible in spite of occurrence of small degradation in image contrast or brightness.

2. Tamper Resistance

Tamper resistance refers to a watermarking system's resistance to hostile attacks. There are several types of tamper resistance. Depending on the application, certain types of attacks are more important than others.

3. Active attacks

In active attacks the hacker tries to remove the watermark or make it undetectable. This type of attack is critical for many applications, including owner identification, proof of ownership, fingerprinting, and copy control, in which the purpose of the mark is defeated when it cannot be detected.

4. Passive attacks

In this sort of attacks, the hacker is not trying to remove the watermark, but is simply trying to determine whether a mark

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

is present, i.e. is trying to identify a covert communication.

5. Collusion attacks

In collusion attacks the hacker uses several copies of one piece of media, each with a different watermark, to construct a copy with no watermark. Resistance to collusion attacks can be critical in a fingerprinting application, which entails putting a different mark in each copy of a piece of media.

IV. WATERMARKING TYPES

Digital Watermark based cyber security system is a technique, in which the secret information called watermark, is capable embedded into the images for preserving the digital images from illicit copying and exploitation. Visible and invisible are the two basic types of Digital Watermark based cyber security system. The example of an evident watermarking technique is watermarking on the bills; here the implanted watermark can be viewed by eyes. The benefit of visible watermarking is that we can identify the proprietor of the watermarking without any calculation, but the drawback is that the embedded watermark can be detached or destroyed quickly. The most common example is the encoded channels on the cable TV. Whereas in invisible watermarking technique, the watermark is concealed in the unknown places in the media data and can't be viewed by our eyes. If someone illicitly exploits the watermarked data, then the embedded watermark will be useful for proving the ownership. As well, invisible watermarking can be classified into two types: robust and fragile watermarks. Generally, robust watermarks are designed to defend against arbitrarily malicious attacks such as image scaling, blending, cropping, lossy compression, and so on. They are frequently employed for copyright protection to proclaim the legal ownership. In contrast, for image authentication, the fragile watermarks are adopted and designed to identify any illegal alterations. A useful Digital Watermark based cyber security system technique has to be indiscernible and robust against common image manipulations like compression, filtering, rotation, scaling, cropping, and collusion attacks among several Techniques.

V. CONCLUSION

This algorithm can be varied depending on the type of application for services being offered. Therefore it is hoped that the future Digital Watermark based cyber security system will play a vital role in cyber security. Helps people to understand cyber watermarking and its importance. Developing countries need to integrate protection measures into the roll-out of the Internet from the beginning, as although this might initially raise the cost of Internet services, the long-term gains in avoiding the losses and damage inflicted by cybercrime are significant and far outweigh any initial outlay on technical protection measures and network safeguard.

REFERENCES

1. Zhu, J, Wei, Q, Xiao, J & Wang, Y 2009, ‘A Fragile Software Watermarking Algorithm for Content Authentication’, IEEE Youth Conference on Information, Computing and Telecommunication, YCICT’09.
2. Zhao Dawei, A, Chen Guanrong, B & Liu 2004, ‘A chaos-based robust wavelet-

domain watermarking algorithm', Chaos, Solitons and Fractals, vol. 22, pp. 47–54.

3. Yashar, N & Saied, HK 2010, 'Fast watermarking based on QR decomposition in wavelet domain', Proceedings of the 2010 sixth international conference on Intelligent information Hiding and Multimedia Signal Processing, pp. 127-130.
4. Veysel Aslantas, A, Latif Do & Serkan Ozturk 2008, 'DWT-SVD Based Image Watermarking Using Particle Swarm Optimizer'.
5. Sujatha, CN & Satyanarayana, P 2016, 'Analysis of Robust watermarking Techniques:A Retrospective' International Conference on Communication and Signal Processing, India, DOI: 10.1109/ICCSP.2016.7754151.
6. Sridhar. B & Arun. C 2013, 'A Wavelet based Image Watermarking Technique using Image Sharing Method', IEEE.