ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

A NOVEL METHOD OF DIGITAL WATERMARKING FORSECURITY ENHANCEMENT IN CLOUD COMPUTING

Swetha.E*, Dr.G.Rosline Nesa Kumari, S.Kaviya
Department of CSE, Saveetha School of Engineering, Thandalam, Chennai, Tamilnadu, India.

Received on 10-08-2016 *Accepted on 06-09-2016*

Abstract

A watermark is specially a kind of information that is embedded with the facts in order to avoid its manipulation, to verify for possession evidence. Widely used watermarking is on still image, videos, and in general on audios. Relying at the kind of information to be watermarked various algorithms are used along with patchwork algorithm used for image watermarking. In this proposed device watermark is embedded with the virtual image and it is saved to the cloud garage. While storing the image the watermark also saved one by one into the storage using personal key. The non-public secret is shared securely to the meant user. Receiver has obtained the personal key. The user get the image and extract the digital watermark from the unique image the usage of the non-public key. To verify that the unique image is tampered or no longer, the usage of the non-public key, retrieve the watermark that is stored into the garage even as storing the watermark embedded image into cloud. Then the consumer verifies that the extracted watermark from authentic image is matched with the retrieved watermark, it's far confirmed that the unique image isn't tampered.

I. Introduction

There are many methods for watermarking image personally or in batch mode for a couple of images. Many image processing and internet gallery generating programs will have the watermarking skills constructed into them and there are also specialized gear designed for watermarking many images immediately [1].In healthcare institutions will adapt cloud based totally for archiving medical images controlled to get right to entry of these information and authentication of images ought to be enforced to mitigate fraudulent sports and clinical errors [2].While the watermark is embedded in the data and stored inside the database. Now while the database is retrieved a unique secret's used with the supply data and on this manner the integrity of facts is accomplished by using verifying in opposition to the integrity of extracted watermark [3]. It facilitates to perceive an outsider; on every occasion the facts

is to be had publically the proprietor of the records would like to restriction the information to any unauthorized user over the community. Every time a data is travelled over the network a wonderful logo is embedded so as to prevent its unlawful use [4]. If at any point of time an illegal reproduction of information is determined, the unique copy may be decided via fingerprinting. If users want to protect images from unauthorized use, including an image watermark to each of them is the fine answer [5]. The image can also contain person call, the logo of images studio or the one of the company which owns the copyrights for the images. It guarantees record security by figuring out important facts and banknotes by including an invisible layer of protection in opposition to unauthorized changes or replica [6]. Watermarks were used for centuries to authenticate images and prevent forgery. Today watermarks are embedded into digital images in order that valid proprietors can assert possession and ensure the validity of their statistics [7]. However, those images (like fingerprints) are being transmitted over channels with accelerated frequency, as a consequence the capacity for attacks all through transmission is a first-rate issue. Recipients need a mechanism that could verify the integrity of their image. If the images are watermarked, it's far trustworthy for the proprietor to authenticate the images [8]. However, determining whether the correct picture has in reality been dispatched and that it has been transmitted without alteration calls for use of facts the owner would prefer not to transmit (particularly the watermark itself or the authentic image). A technique for setting up the identity of an individual is important in all transactions whether they're industrial or personal. The capability to set up identity with certainty can save you fraud or forgery. inside the midst of an digital revolution, this remains a main concern in e commerce, telecommunications, healthcare, and safety [9]. At the same time as verifying the identity of people has usually been a situation, in the beyond, it turned into generally dealt with facts such as a social safety number or a password, or some type of physical key like an identification card. But, these methods are steadily dropping choose and are being replaced by means of biometrics parameters, such as fingerprint, speech and iris, which can be "unique" to an character and in order that those watermarks can't be without problems altered. Cloud computing is computing that is based on the net and it is a maximum current fashion in IT global [10]. In cloud computing shared information sources and software program which can be imparting to computer systems and lots of different gadgets on call for. Electronic mail changed into probable first carrier on the “cloud”. In cloud computing, the cloud provider companies (CSPs), inclusive of Amazon, are able to deliver various services to cloud users with the assist of effective facts center. One of the most essential offerings provided by cloud vendors is statistics storage [11]. Let us do not forget a practical data utility. A business enterprise lets in its staffs inside the identical institution or department to keep and share files

in the cloud. Cloud is a generation based on net that uses the net and principal far off servers to support data or image and applications [12]. By means of using the cloud, the staffs can be absolutely released from the toughest nearby statistics garage and preservation. However, it also poses a substantial change to the confidentiality of those saved documents. In particular, the cloud servers managed by cloud providers are not absolutely trusted by users wish the data documents stored inside the cloud can be sensitive and confidential, such as enterprise plans [13]. In Cloud computing due to community site visitors make network bandwidth greater green which brought cloud to each infrastructure and server. With the assist of Cloud Computing, customers can access their databases from everywhere inside the global only if they connected to the internet [14]. Today's international relies upon on cloud computing to save their public data as well as non-public statistics. That data or image may be required by using them or others at the spot of time. As a end result, data or image safety in cloud computing has required lots of interest from the studies society. Amazon played active function in this. IBM, google, many universities and groups followed it [15].

II. Related Works

The cause of watermarks is -fold: (i) they may be used to decide possession, and (ii) they may be used to locate tampering. There are two essential features that each one watermarks have to own. First, all watermarks need to be detectable. If you want to determine possession, it's miles vital that one be capable to get better watermark. There are basically two mechanisms by way of which a watermark can be recovered. Incomplete watermarks can only be recovered by providing the unique photo available. Entire watermarks can be recovered regardless. Whole watermarks are extra desirable as they observe to a broader spectrum of packages. When watermarking massive documents or a huge wide variety of documents in a database, complete watermarks are top-rated as they make it pointless to store a couple of copies of the authentic (unwatermarked) report. 2nd, watermarks must be robust to numerous styles of processing of the sign (i.e. cropping, filtering, translation, compression, etc.). If the watermark isn't always strong, it serves little cause, as possession will be misplaced upon processing. However, having a few integrated fragileness can be beneficial at times [16].

If fragile watermarks are used and the information is altered, the watermark can pinpoint the areas that have been modified. Fragile watermarks can discover minor modifications or tampering of records. strong watermarks however, are beneficial for detecting big-scale assaults on data. One capability hazard with touchy databases containing biometric identifiers is that they're in all likelihood to be attacked by means of hackers or criminals. Watermarking the records in those databases can allow the integrity of the contents to be validated. But any other danger is that this

critical records may be attacked while it's far being transmitted. As an example, a 3rd celebration should intercept this statistics and maliciously regulate the records before re-transmitting it to its very last vacation spot. The transmission hassle is even more crucial in cell and wireless channels [17].

III. DWT with Least Significant Bit

Discrete Wavelet transform (DWT) is a mathematical device for hierarchically decomposing an image . It's far useful for processing of non-stationary signals. The transform is based totally on small waves, called wavelets, of various frequency and confined period. Wavelet transform presents each frequency and spatial description of animation image. Wavelets are created with the aid of translations and dilations of a fixed function referred to as mother wavelet. DWT is the multi resolution description of an image the interpreting can be processed sequentially from a low decision to the higher decision [18]. The DWT splits the sign into high and low frequency parts. The high frequency part carries data approximately the edge additives, at the same time as the low frequency element is split once more into excessive and low frequency elements. The high frequency components are normally used for watermarking for the reason that human eye is less sensitive to adjustments in edges. In dimensional programs, for every level of decomposition, we first perform the DWT in the vertical course, observed by using the DWT in the horizontal route. After the primary stage of decomposition, there are four sub-bands: LL1, LH1, HL1, and HH1. For each successive degree of decomposition, the LL sub-band of the previous level is used because the center. To perform 2nd degree decomposition, the DWT is carried out to LL1 image Watermarking the use of 3-level Discrete Wavelet transform (DWT). To perform third level decomposition, the DWT is applied to LL2 band which decompose this band into the four sub-bands – LL3, LH3, HL3, HH3. This results in 10 sub-bands in line with component. LH1, HL1, and HH1 incorporate the best frequency bands gift in the image tile, at the same time as LL3 carries the bottom frequency band. fig1 shows the working methods of DWT [19].

IV. Proposed Method

The Architecture of the proposed system diagram of Fig 2 consists of several components such as sender, receiver, cloud server, cloud storage, watermark embedded image.

- Sender: Sender embedded watermark with the original image and upload the watermark image into the cloud storage using private key.
- Receiver: Receiver will extract the embedded watermark image using the private key, which is shared among the sender and receiver. From embedded watermark image receiver will extract the watermark image, then

compare the extracted watermark image with the retrieved original image from cloud storage. If third party has made any changes in the image, then there will be difference between the extracted watermark image and retrieved watermark image.

- Cloud server: Cloud servers suggest digital servers which run on cloud computing environment. this is why very regularly Cloud Servers are called virtual disk service(VDS). While it's far genuine that each cloud server may be known as a digital dedicated server, the alternative is not usually real. That is because a digital committed server can be located simplest on a unmarried hardware server and for this reason be afflicted by a unmarried factor of failure while any of its hardware fails. Cloud servers run as software-unbiased devices. Which means a cloud server hasall the software program it calls for to run and does not depend on any centrally-set up software program.

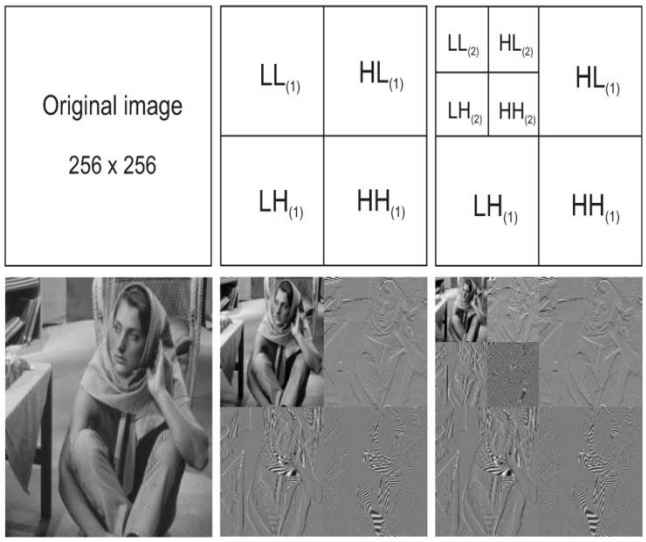

Fig-1.

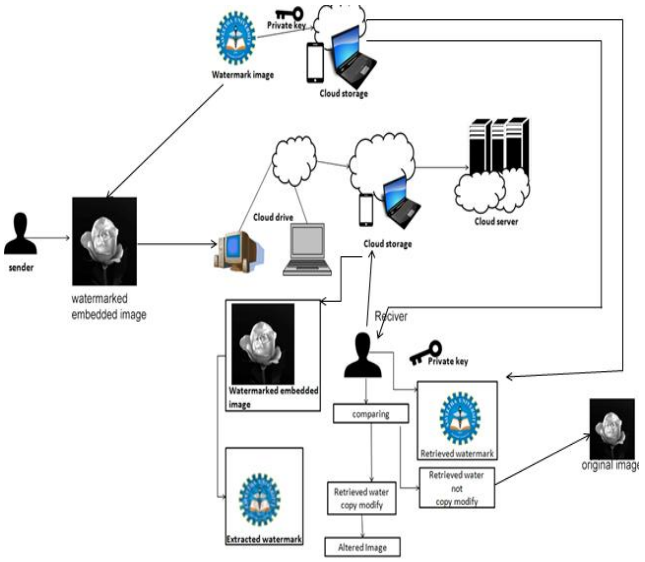

Fig-2.

A watermarking algorithm embeds watermark in one-of-a-kind type of statistics like, text, audio, video etc.. The embedding procedure is accomplished by means of use of a private key which determined the locations inside the multimedia image where the watermark might be embedded. Once the watermark is embedded it can happens several assaults because the on line object may be digitally processed. The attacks can be unintentional, hence the watermark must be very sturdy in opposition to all assaults that is feasible. When the owner wants to test the watermarks inside the attacked and damage multimedia image, sender depends on the personal key that was used to embed the watermark. Using the secrete key, the embedded watermark may be detected. This detected watermark might also or may not combine the unique watermark due to the fact the image could have been attacked. Therefore to validate the presence of watermark, the original records is used to evaluate and extract the watermark signal (non-blind watermarking) or a correlation method is used to locate the strength of the watermark sign from the extracted watermark (blind watermarking). In the correlation, detected watermark from the authentic statistics is in comparison with the extracted watermark.

V. Result

This paper describes about the conversion of normal image into watermarking image. The original image or normal image has been retrieved to get the extracted watermarked image. An extracted watermarked image is that which will not be clear or a blurred image. The sender will send the private key to the receiver so that the receiver can get the watermarked image by using the private key. One major flaw in this method is its inability to detect whether the alterations in the image are due to channel distortions and noise or actual tampering by an individual. The transmission noise is a rather difficult task since it cannot always be modeled as a white noise effect. Sometimes the transmission noise is a function of the encoding scheme employed, and at other times it is a function of the channel itself.

VI. Conclusion

Watermarking in digital image is a still are relatively new issue, but it is of growing importance as more robust methods of verification and authentication are being used. However, it is only a semi-unique key. It is possible to alter the image yet retain the same key, as the average is not always the best tool for characterizing data. Such a problem could be solved by exploring alternate ways of characterizing data. One major flaw in this method is its inability to detect whether the alterations in the image are due to channel distortions and noise or actual tampering by an individual. Unfortunately, attempting to factor out transmission noise is a rather difficult task since it cannot

always be modeled as a white noise effect. Sometimes the transmission noise is a function of the encoding scheme employed, and at other times it is a function of the channel itself. However, having a way to determine whether the "tampering" is the result of noise or a malicious attack would be useful. Ultimately though it is not that necessary. In order for the noise to be seen as tampering, it must be strong enough to. Start disrupting the image and from that point on it could be interpreted as an accidental attack. Another potential problem is the "disgruntled employee" attack. If a disgruntled employee has access to the executable, then it is straightforward to make the executable always agree that the image received has not been tampered even if it has been. Similarly, the executable could be altered so that it gives consistently negative responses. Thus, there needs to be some way to prevent such attacks. One way to do so would be to introduce a random function that operates in conjunction with the executable, so that for example, a 5x5 local average key is not the only possibility.

References

1. R.G. Van schyndel, A.Z. Tirkel, and C.F. Osborne."A digital watermark", in complaints of the IEEE global convention on photo processing, vol.ii, pp. 86-90, 1994.
2. I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon. "Watermarking for multimedia", NEC studiesinstitute technical file, ninety five-10, 1995.
3. Ronald l. krutz, "Cloud computing basics", what's cloud computing, indianapolis, indiana, 2010,ch.1, sec.1, pp.26, 30-32.
4. C. Hsu and j. wu."Hidden signatures in photographs".IEEE ICIP iii 'ninety six, pp. 223-26.
5. Russell dean vines, "Cloud computing software program security fundamentals", indianapolis, indiana, 2010, ch.3, sec.1, pp.ninety.
6. Amandeepverma, Sakshikaul, "Cloud computing safety issues & demanding situations: a survey", springer verlag berlin heidelberg, part iv, CCIS 193, pp.445-454, 2011.
7. Ronald l. krutz, "Cloud computing software security basics", cloud records security objectives, indianapolis, indiana, 2010, ch.3, sec.1, pp.ninety one-ninety two.
8. Zhiguo du, Da Huihu, "Photograph watermarking technology based on cloud version", asia pacific young people convention on verbal exchange technology, pp.25.27, 2010.
9. Agostinocortesi, Shantanu friend, "Watermarking techniques for RBD: survey class & evaluation", journal of commonplace laptop technology, vol.sixteen, no.21, pp.3164-3171, 2010.

10. Akhilbehl, "Rising safety challenges in cloud computing", global congress on data and communication era, pp.217-218, 2011.
11. Wayne jansen, "Suggestions on safety & privacy in public cloud computing", special e-book 800-144, national institute of standards & generation.
12. Joshiakshay "enhancing security in cloud computing", information &; knowledge management, vol.1, no.1, pp.40-43, 2011.
13. Cyril bazin, jean marie, "A unique framework for watermarking", springer-verlag berlin heidelberg, pp.201 217, 2008.
14. Priyankaarora, Himanshutyagi, "Evaluation and assessment of protection problems on cloud computing environment", global of computer technology and statistics generation magazine, vol.2, no.five, pp.179-183, 2012.
15. Yong zhang, Xiamuniu, " A method of protecting RDB copyright with cloud watermarking", world academy of science, engineering & technology, pp.68.72.
16. Cong Wang, Qian Wang, and KuiRenWenjing Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, 978-1-4244-5837-0/10/$26.00 ©2010 IEEE.
17. Ryan K. L. Ko, Markus Kirchberg, Bu Sung Lee , From System-centric to Data-centric Logging Accountability, Trust & Security in Cloud Computing.
18. L. Sumalatha, G. RoslineNesaKumari, V. Vijaya Kumar, "A simple block based content watermarking scheme for image authentication and tamper detection", International Journal of Soft Computing and Engineering (IJSCE), pp. 113-117, 2012.
19. G.RoslineNesaKumari, L.Sumalatha and V.Vijayakumar, "Fuzzy Based Chaotic and Logistic Method for Digital Watermarking Systems",International Journal of Scientific & Engineering Research Vol. 3, 2012.