Integrity Watermarking and QR-Code Techniques for ensuring Printed Document Authenticity Real Time Distribution

MISNI HARJO SUWITO†[1]1, YOSHIFUMI UESHIGE†[2]2
YAOKAI FENG† [3]3, KOUICHI SAKURAI†[4]4.

Abstract: Discussion on protection, authentication, and validation scheme of digital documents is very challenging. This current almost community using the Information and Communication Technology. And this technology developed very rapidly and very convenient to get information. On the other hand, they are also disadvantages digital document forgery remains a serious issue such as passports, transcript, diploma certificates, etc. This paper proposes a novel document authentication scheme applying digital watermarking and QR-Code. In this scheme owner of the document will insert a logo to validate and verify documents or distribution connected to the web server the result of this scheme technique validating can be performed in real time by using the smartphone. With this scheme is expected to verify the documents and can be implemented in all organizations, government, education, higher institution, and business sectors are optimized.

Keywords: Watermarking; QR-Code; Discrete Wavelet Transform, Document Authentication; Security; Protection; Document Link Validation

1. Introduction

With the Internet developing rapidly as it is today, the user document still playing a role that cannot be underestimated. The printed document authenticity is physically needed by a human in daily life as well as the contents document information must be protected from threats and attacks such as alteration, deletion, unauthorized modification.

The Diploma is a printed document that is protected by law in each country and has the law force. And this is an authentic proof that someone has completed their education have been taken. Currently, most of the Diploma is still stored in the form of printed paper, so there is a chance it can be forged by other parties who are not responsible. Therefore, the protection document authenticity printed is very important.

Diploma normally used to apply for a job or continue their education to a higher level. Many institutions and people feel very worried about the diploma authenticity applicants. To verify the diploma authenticity diplomas usually by calling and emailing the responsible publisher gets a diploma. There are several ways to verify the authenticity of the certificate, first by utilizing Quick Response Code (QR-Code). Utilization of QR-Code technology can verify the certificate's authenticity and Security this had been done earlier researchers [1]. so that it can quickly know the result.

However, these methods are still weaknesses. Both resolve this problem, watermarking can be proposed as one solution. Digital watermarking is a method for copyright protection for multi-media. This method can also be used to verify the digital document authenticity. In verifying digital watermarking documents may show performance abilities to withstand surgery and image manipulation are done, such as JPEG compression and the addition Gaussian [2]

Digital watermarking used in the digital image is always developed with the aim to achieve watermarking techniques that have criteria there are robustness, imperceptibility, and security of the original image [3]. (1) Robustness is resistance to efforts to eliminate the watermark and resistance to operation image or attack. (2) Imperceptibility is insertion is not arousing suspicion observation of the senses of human sight. (3) Security is the insertion which cannot be detected by statistical analysis or Other methods [4]. Some watermarking techniques discovered by researchers. Watermarking first published in 1979, using techniques, spatial domain called Least Significant Bit (LSB) [4]. LSB techniques contained in [5] and [6]. Apostol [7] proposed digital watermarking using PWLCM and insertion LSB. LSB technique very vulnerable to many attacks [8].

In the domain of transformation, a technique widely used Cosine Transform Discrete (DCT) [9], and Transformation Discrete Wavelet (DWT) [10]. DCT can split the image into several parts. However, this technique requires a long time for operations [11]. On the other hand, DWT has many also used for watermarking because of the multi-resolution capability he [12]. Nevertheless, DWT also has shortcomings, such as shift sensitivity and poor directionality [13].

DWT and DCT hybrid technique [14]. the main idea of hybrid is that combine both of these techniques can cover the shortfall respectively, so that the watermarking scheme more effective [15]. Therefore, the most excellent technique that is inserting a watermark is at the centre frequency [16]. Discrete Wavelet

[1] Kyushu University
[2] Nagasaki University
[3] Kyushu University
[4] Kyushu University

Transform (DWT) - Discrete Cosine Transform (DCT) [11], Singular Value Decomposition (SVD) - Discrete Wavelet Transform [18], Redundant Discrete Wavelet Transform (RDWT) - Singular Value Decomposition [19] and Combining Techniques Discrete Wavelet Transform (DWT) - Discrete Wavelet Transform (DWT) - Discrete Wavelet Transform (DWT) [20].

For the method, above-mentioned is a system that is able to verify the digital certificate authentication using the watermarking technique.

QR-Code method to hide the versatile because it has flexible criteria, structure, and diverse that a lot of researchers to increase the data storage capacity, security applications such as various types of watermarking.

This paper proposes a novel scheme authentication techniques using integrity watermarking and QR-Code. In the method described in the first document encryption in a random matrix, then it will not be a visible watermark on the cover of the document and it does not look the information contained in the document. From the documents that have been watermarked then, will be encrypted with a QR-Code, so that the watermarked document is no longer recognizable, and thus more secure. To be able to look back at the original document with the means to decrypt.

The main contribution of this paper are following:

- To reduce the risk level of the original document falsification of counterfeiters;
- To provide security to the original document that is stored with a model of digital documents;
- To verify the document authenticity in real time, effectively and efficiently.

This paper organized as follows; introduction several techniques as digital watermarking and QR-Code, in Section 2 Literature Review, Section 3 Proposed Method, Discussion and result in Section 4, and the finally conclusion in Section 5.

2. Literature Review

The physical document was used to print important papers such as certificates, diplomas, academic transcripts, cooperation contracts, agreements, and certificates of land ownership. However, several cases of forgery of printed documents have been found in recent years. Created false documents to deceive people who do not pay attention to the authenticity of the original document. One US official made embarrassed when important reports received stating Iraq was developing weapons of mass destruction, is a report that has been falsified. In another case, two police officers were detained for some time because it has changed the affidavit witnesses, and using the false letter to the office of the Criminal Investigation Department (Criminal Investigation Department - CID) in Malaysia [21]. Forgery and manipulation of documents can cause a significant loss in terms of the trust relationship, as well as the validity of a physical document. The action is essential, to ensure a document to avoid the implications of important documents, conducted by the parties without interest. Counterfeiting usually divided into two types: forgery by issuing a similar document, and forgery by using a scanner and a printer from an original document [22].

Verification of documents necessary to ascertain the file authenticity and to prove who is the legal document owner. Verification can be done in several ways. For instance, text integrity verification documents sent by fax, using the technique of pixel reorganizing. This technique was proposed [23] by using a camera to take the document image sent by fax. Documents examined and verified by MAC algorithm, to detect the text content is there has changed. The results show that the proposed method successfully detects text that has been changed despite different font sizes. Similar methods are also used [24]. This research not only documents emanating from the observed fax machine but also documents that are processed via fax and internet device.

Determining a document such as a diploma is genuine or fake is a challenging job. Globally verification of digital documents using watermarking aims to examine the object authenticity, including digital certificates. A message can be text or digital image pasted into a digital certificate. These watermarks can be either visible or invisible watermark. This message can be extracted or retrieved from a digital certificate. If the message is extracted together with the insertion message, it means that the digital certificate is authentic or official diploma. Conversely, if the message is extracted in contrast to the inserted, or the message has been distorted, meaning there is a possibility that the digital certificate has been manipulated by unauthorized parties. Research on the use of watermarking for verification of documents was made [25]. Yin inserts the invisible watermark into the digital photo with a diploma owner insertion force that varies based on the characteristics of the Human Vision System (HVS). Watermarking for digital images proving ownership investigated [26]. Watermarking for digital images proving ownership investigated. Experiments show that the proposed method is effective, and can withstand an attack on the digital image is done. Verification of digital documents using a combination of watermarking and hashing proves a significant achievement. The method proposed [27] can withstand the operation compress JPG with a compression rate of 60 as well as some other image manipulation.

2.1 Security and Protection

Security, in information technology (IT), is the defence of digital information and IT asset against internal and external, malicious and accidental threats. This defence includes detection, prevention and response to threats through the use of security policies, software tools, and IT services. Security Data refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases, and websites. Data security also protect data from corruption. Data Security is the main priority for organization of every and genre. Also on personal data security is also a major issue, such as passports, assurance, bank accounts, diploma, and transcript.

2.2 Validation Link of Document

Document Validation link is associated with the network address or the address where the site gets a response from the server and will show the authentication of documents. This service can be requested through the query data from a web server, so authentication of the information and will show the results of authentication on mobile devices.

Application of the QR-Code contains characters that are already embedded in the application system would generate a QR code and corresponding process and it is a standard that has been set. Link validation document is a character that has been implanted in the QR-Code system. These links will automatically connect to the web address via an Internet connection to check the authenticity of the data.

2.3 Document Authentication

Document Authentication is the process of verifying the official purpose of a document so that it can be accepted at the face value by officials in another country. Various documents such as (passport, insurance, bank account, single identity number, land titles, birth /death certificate, marriage/divorce certificate, official letter, transcript, and diploma certificate, etc.) submitted to this office are being used internationally for adoptions, dual citizenship, doing business, transferring school records, etc. Documents Authentication has been approved and can be used in all other nations are authenticated by what is called a "certificate of office".

3. Proposed Method

Watermarking techniques have been widely used in preserving document copyright and authenticity. Watermarking can be applied in both digital format and printed form. Like steganography, watermarking employs the concept of data hiding into media such as image, audio and text where watermarking emphasize more on robustness instead of the ability of not being perceived by human visual and auditory.

3.1 Integrity Algorithm Watermarking and QR-Code

This scheme a novel technique to integrate the watermarking with QR-code to protect the document authenticity in real time. Integrity processes can be seen Figure 1.

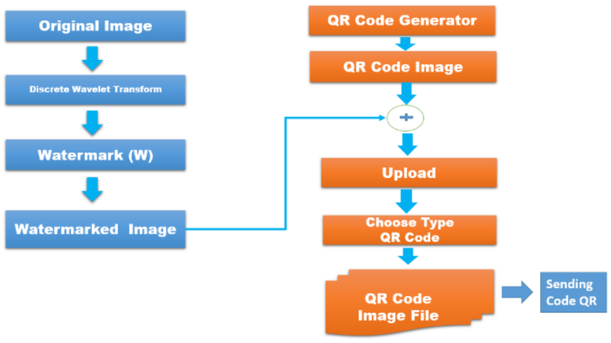

Figure 1. Integrity Processes Watermarking and QR-Code Algorithm

The process of watermarking techniques based on Discrete Wavelet Transform. The process of image embedding and image extraction. After processing will be embedded into the three-layer wavelet transformed the diagonal component.

To validation the scheme is on shown as in figure 6, the synchronization is using internet connection and will be contacting a web server and database server for checking link request, scheme printed document authentication are detail as follows:

A. The scheme generating and embedding

- To Generate scan watermarked QR-Code including document validation link distribution which has prepared web server and database server.
- To Embed watermarked QR-Code into distribution document

B. The scheme for Authentication

- To Scan watermarked QR-Code using QR-Code reader
- Go to internet link provided
- Check the internet link with the web server and database server provide previously.
- Finally printed the document.

3.1.1 Watermark Image Embedding

The process embedding, Step 1, apply 3 levels DWT on host image decomposes the image into sub-image, 3 detail and 1 approximation. The technique alpha blending [28, 29, 30] is used to insert the watermark in the host image. This technique the decomposed components of the host image and the watermark are multiplied by scaling factor and added.

Alpha blending: Formula given by

MWI=k(LL3)+q(WM3)

Where WM3= low frequency approximation of watermark.

LL3= low frequency approximation of the original image, MWI=Watermarked image, k, q-Scaling factors.

Step 2, After embedding the watermark Image on cover image coefficient to generate the final secure watermarked image. Figure 2.

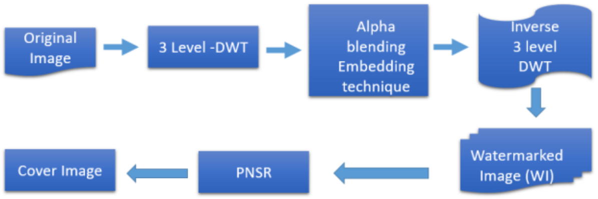

Figure 2 The watermark embedding process diagram

3.1.2 Image Extraction

The process embedding, Step 1, apply 3 levels Discrete Wavelet Transform to watermarked image which decomposed the image in sub-bands. Step 2, After this apply alpha blending on low frequency components.

Alpha blending: Formula extraction for recover watermark given by

RW= (MWI-k*LL3)/q

Where RW=low frequency approximation of recovered watermark, LL3=low frequency approximation of the original image, and WMI= low frequency approximation of watermarked image.

Step 3, After extraction process, Inverse Discrete Wavelet Transform is applied to the watermark image coefficient to generate the final watermark extracted image. Figure 3.

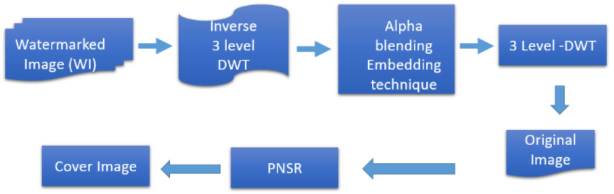

Figure 3. The watermark extraction process DWT diagram

3.2 2-Dimensional Code (QR-Code)

QR-Code is Quick Response Code. It has already overtaken the classical barcode in common popularity in many areas because of several advantages. It was developed by Denso Wave in 1994, one of Toyota automobile cooperation group. It has approved by International Standard (ISO/IEC 18004) 2000. QR-Code is capable of representing the same amount of data in approximately one-tenth the space of traditional barcode [31]. While QR-Code capacity, up to 7,089 (Numerical), 4,296 (Alphanumerical), 2,953 (Binary/Byte), 1,817 (kanji/kana) characters can be encoded in one symbol. QR-Code consist of black and white modules which represent the encode data.

3.2.1 Encoding Process Algorithm

The process encoding using 2-Dimensional code. After embedded image (watermarked) than upload into 2-Dimentional code generator application. The procedures as follows:

- Step 1, Open en.qrcode-pro[33]
- Step 2, Select QR-Code generator
- Step 3, Browse image original
- Step 4, Select QR-Code model/design
- Step 5, Select encode
- Step 6, Select preview to showing QR-Code
- Step 7, Select Finish/save

3.2.2 Decoding Process Algorithm

- Step 1, Open en.qrcode-pro[33]
- Step 2, Select QR-Code reader
- Step 3, scan qrcode
- Step 4, preview original image
- Step 5, Finish

4 Discussion and Result

Discrete Wavelet Transform (DWT) is a transformation the discrete signal into wavelet coefficients obtained by filtering the signal with two different filters that filter low and high filter. discrete Wavelet Transform (DWT) split (decompose) digital images into 4 sections at a frequency sub-band that image. Components sub-band wavelet transformation generated by lowering the level of decomposition. Discrete Wavelet Transform (DWT) can be done by passing a signal via a Low Pass Filter (LPF) and do down-sampling the output of each filter [32].

Wavelet transform provides both frequency and spatial description of an image. Its multi-resolution analysis (MRA) the signal at different frequencies giving different resolution. Discrete Wavelet Transform is very suitable to identify the areas in the cover image where the secret image can be embedded.

Discrete Wavelet Transform [34] first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For next step, 2 level of decomposition there are 4 sub-bands: LL2, LH2, HL2, HH2, and the finally in 3 level of decomposition, there are 4 sub-bands also: LL3, LH3, HL3 and HH3. Figure 4.

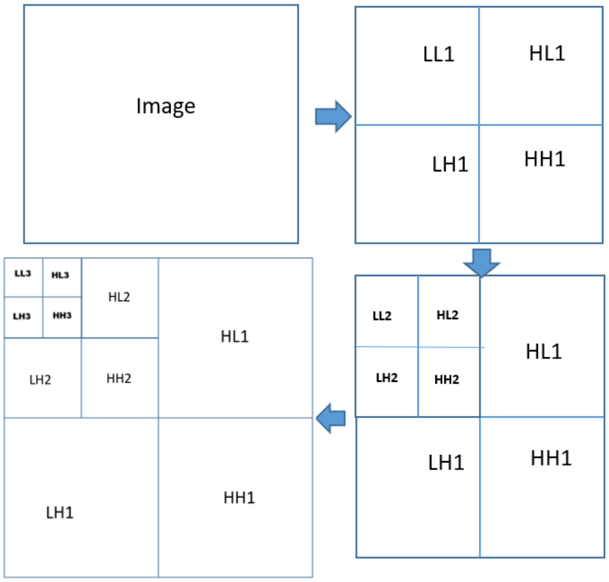

Figure 4. The 3 level of Discrete Wavelet Transform Decomposition

In this scheme, watermark embedding algorithm using DWT decomposition. The watermark information after processing will embedded into three-layer wavelet transformed the diagonal components, which reduces the influence from the image watermarking to the QR-Code. The watermark information is a binary image. QR-Code are generated by software. The watermark embedding procedure as follows and for process shown in figure 5.

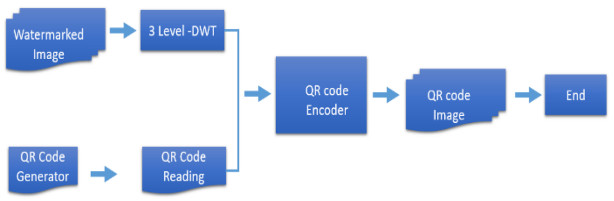

Figure 5. The flow process watermark and QR-Code diagram

To capture the QR-Code at this time so many applications available on within the smartphone is equipped with a high-resolution camera and other features that can support it. Smartphones today with a variety of operating system is developing very fast, everything can be a solution that can simplify the job.

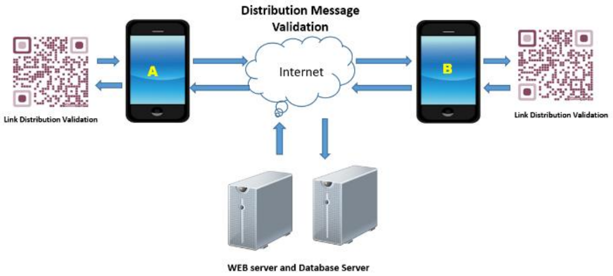
Distribution Message Validation
Internet
A
B
Link Distribution Validation
Link Distribution Validation
WEB server and Database Server

Figure 6. Document Authentication Real Time Distribution

With a smartphone some applications can install such as a QR-Code reader. The smartphone is equipped with a QR-Code generator, QR-Code scanner, and reader, etc. Features in the smartphone are also equipped with a webcam, this at the same time will also be able to read link for validation, directly connected to the internet to the web server and database server will send a message that has been validated.

5 Conclusion

Based on the result, authentication document though integrity watermarking and QR-Code implemented. As the smartphone become an indispensable accessory and carry-on device in real life, compared with the traditional key or access card, sending the authentication document or image in real time. Watermarking and QR-Code technology continues to evolve. Opportunities for future Watermarking technology is promising. Challenges and obstacles to realizing this dream a lot, all the power and effort has been expended to overcome these challenges. Therefore, we should be able to explain the important aspects of the future of technology will watermarking.

For future research watermarking and QR-code can be developed is to address some of the attacks on the digital document and embedding multimedia such as Unauthorized Embedding, Unauthorized detection, Unauthorized Removal, and System Attack.

Reference:

[1.] Alam, M., Badawy, W., & Graham, J. (2005). A new time distributed DCT architecture for MPEG-4 hardware reference model. IEEE Transactions on Circuits and Systems for Video Technology,15(5),726–730. doi:10.1109/TCSVT.2005.846429

[2.] Al-Haj, A. (2007). Combined DWT-DCT Digital Image Watermarking. Journal of Computer Science, 3(9), 740–746.

[3.] Bamatraf, A., & Ibrahim, R. (2010). Digital Watermarking Algorithm Using LSB. 2010 International Conference on Computer Applications and Industrial Electronics, 155–159.

[4.] Beusekom, J. Van, & Shafait, F. (2011). Distortion Measurement for Automatic Document Verification. 2011 International Conference on Document Analysis and Recognition, 289–293. doi:10.1109/ICDAR.2011.66

[5.] Fernandes, F. C. A., Spaendonck, R. L. C. van, & Burrus, C. S. (2003). A New Framework for Complex Wavelet Transforms. IEEE Transactions on Signal Processing, 51(7), 1825–1837. doi:10.1109/TSP.2003.812841

[6.] Gui, G., Jiang, L., & He, C. (2006). A New Watermarking System for Joint Ownership Verification. Proceedings 2006 IEEE International Symposium on Circuits and Systems, 2006., 5756–5759.

[7.] Hajjara, S., Abdallah, M., & Hudaib, A. (2009). Digital Image Watermarking Using Localized Biorthogonal Wavelets. European Journal of Scientific Research, 26(4), 594–608.

[8.] Kong, I.-K., & Pun, C.-M. (2008). Digital Image Watermarking with Blind Detection for Copyright Verification. 2008 Congress on Image and Signal Processing, 504–508. doi:10.1109/CISP.2008.546

[9.] Lai, C., Wang, W., & Jhan, C. (2010). Improved DCT-Based Watermarking through Particle Swarm Optimization. Proceedings of the Second International Conference on Computational Collective Intelligence, 21–28.

[10.] Lee, G.-J., Yoon, E.-J., & Yoo, K.-Y. (2008). A New LSB Based Digital Watermarking Scheme with Random Mapping Function. 2008 International 33 Symposium on Ubiquitous Multimedia Computing, 130–134. doi:10.1109/UMC.2008.33

[11.] Maity, S. P., & Kundu, M. K. (2001). Robust and Blind Spatial Watermarking in Digital Image. Tech. Rep., Dept. of Electronics and Telecomm., India.

[12.] Mohamed, M. A., Abou-Soud, M. E.-D. A., & Diab, M. S. (2009). Fast Digital Watermarking Techniques for Still Images. International Conference on Networking and Media Convergence, 122–129. doi:10.1109/ICNM.2009.4907202

[13.] Mohanty, S. P., Ramakrishnan, K. R., & Kankanhalli, M. S. (2000). A DCT Domain Visible Watermarking Technique for Images. 2000 IEEE International Conference on Multimedia and Expo. ICME2000., 1029–1032. doi:10.1109/ICME.2000.871535

[14.] Pramoun, T., & Amornraksa, T. (2013). Text integrity verification for faxed document using pixel reorganizing technique. 2013 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, 1–6. doi:10.1109/ECTICon.2013.6559642

[15.] Premaratne, P., & Safaei, F. (2007). 2D Barcodes as Watermarks in Image Authentication. 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007), (Icis), 432–437. doi:10.1109/ICIS.2007.2

[16.] Rafigh, M., & Moghaddam, M. E. (2010). A Robust Evolutionary Based Digital Image Watermarking Technique in DCT Domain. 2010 Seventh International Conference on Computer Graphics, Imaging and Visualization, 105–109. doi:10.1109/CGIV.2010.24

[17.] V. M. Viswanatham, “A Hibrid Digital Watermarking Algorithm for color images based on DWT-DCT,” Anale Serial Informatica VIT University, School of Computing Science and Engineering, vol. 1, no. 1, pp. 27–33, 2012.

[18.] S. Sirmour and A. Tiwari, “A Hybrid DWT-SVD Based Digital Image Watermarking Algoritthm for Copyright Protection,” International Journal of P2P Network Trends and Technology (IJPTT), vol. 6, pp. 7–10, 2014.

[19.] S. Padhihary, “Digital Watermarking Based on Redundant Discrete Wavelet and Singular Value Decomposition,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 2, pp. 431–434, 2013.

[20.] E. Y. Hidayat and E. D. Udayanti, “Hybrid Watermarking Citra Digital Menggunakan Teknik Dwt-Dct Dan Svd,” Seminar Nasional Teknologi Informasi & Komunikasi Terapan, vol. 1, 2011.

[21.] Salleh, M., & Yew, T. C. (2009). Application of 2D Barcode in Hardcopy Document Verification System. Proceedings Third International Conference and Workshops, ISA 2009, 5576, 644–651

[22.] Beusekom, J. Van, & Shafait, F. (2011). Distortion Measurement for Automatic Document Verification. 2011 International Conference on Document Analysis and Recognition, 289–293. doi:10.1109/ICDAR.2011.66

[23.] Pramoun, T., & Amornraksa, T. (2013). Text integrity verification for faxed document using pixel reorganizing technique. 2013 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, 1–6. doi:10.1109/ECTICon.2013.6559642

[24.] Thongkor, K., Pramoun, T., Chaisri, C., & Amornraksa, T. (2012). Integrity Verification Method of Thai Content for Faxed Document. 2012 9th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 6–9.

[25.] Yin, H., Liang, H., & Niu, X. (2009). A Robust Digital Watermarking Scheme and Its Application in Certificate Verification. 2009 International Conference on Measuring Technology and Mechatronics Automation, 410–413. doi:10.1109/ICMTMA.2009.295

[26.] Gui, G., Jiang, L., & He, C. (2006). A New Watermarking System for Joint Ownership Verification. Proceedings 2006 IEEE International Symposium on Circuits and Systems, 2006., 5756–5759.

[27.] Vasu, S., George, S. N., & Deepthi, P. P. (2012). An Integrity Verification System for Images Using Hashing and Watermarking. 2012 International Conference

[28.] Akhil Pratap Shing, Agya Mishra, Wavelet Based Watermarking on Digital Image, Indian Journal of computer Science and Engineering, 2011

[29.] Nilanjan Dey, Anamitra Bardhan Roy, Sayantan Dey, A novel approach of color image hiding using RGB color planes and DWT, International Journal of Computer Applications, 2011.

[30.] S.MaruthuPerumal Dr.V.VijayaKumar A Wavelet based Digital Watermarking Method using Thresholds on Intermediate Bit Values International Journal of Computer Applications February 2011

[31.] http://www.qrcode.com/

[32.] S. Lagzian, M. Soryani, and F. Fathy, “Robust watermarking scheme based on RDWT-SVD: Embedding Data in All subbands,” IEEE, vol. 1, pp. 48–52, 2011.

[33.] http://en.qrcode-pro.com/Generator

[34.] Nikita Kashyap Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT) I.J.Modern Education and Computer Science, 2012, 3, 50-56 Published Online April 2012 in MECS.