Volume 8, No. 3, March – April 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Analysis on the Algorithm for Cryptography Based MSLDIP Watermarking

Dr. Mohammad Miyan
Associate Professor, Shia P. G. College, University of Lucknow
Sitapur Road, Lucknow-226020.

Abstract: The enhancements in net technologies and growing requests on on-line multimedia system businesses have created digital copyrighting as a big challenge for businesses that are connected with on-line content distribution via various business models together with the rate of pay per view, subscription, trading, etc. The copyright protection and therefore the proof for rightful possession are the major problems connected with the distribution of any digital pictures. The digital watermarking is one in all the instructed solutions for the copyright protection of multimedia system knowledge. This system is best than Digital Signatures and different ways as a result of it doesn't rise overhead. In the present paper there's associate analytical survey on the Cryptography primarily based MSLDIP Watermarking Algorithm.

Keywords: Algorithm, Cryptography, Encryption, MSLDIP, Watermarking.

I. INTRODUCTION

The cryptography before the trendy age was effectively similar with the encryption, the conversion of knowledge from a legible state to apparent nonsense. The conceiver of associate encrypted message shared the coding technique required to recover the initial data solely with supposed recipients, thereby precluding unwanted persons from doing identical. The cryptography literature usually uses Alice "A" for the sender, Bob "B" for the supposed recipient, and Eve "eavesdropper" for the opposer. Since the event of rotor cipher machines in war-I and therefore the advent of computers in war-II, the strategies wont to perform cryptanalysis became a lot of advanced and its application more widespread [1].

The current cryptography is much supported the mathematical theory and engineering science practice; cryptological algorithms are designed around the procedure hardness assumptions, creating such algorithms exhausting to interrupt in observe by any opposer. It's on paper doable to interrupt such a system, however it's unworkable to try and do thus by any familiar sensible means that. These schemes are thus termed computationally secure; theoretical advances, e.g., enhancements in number resolution algorithms, and quicker computing technology need these solutions to be regularly tailored. There exist information-theoretically secure schemes that demonstrably cannot be broken even with unlimited computing power-an example is that the one-time pad-but these schemes are tougher to implement than the most effective on paper breakable however computationally secure mechanisms [2], [3].

The growth of cryptological technology has raised variety of legal problems within the modern era. Cryptography's potential to be used as a tool for spying and infraction has crystal rectifier several governments to classify it as a weapon and to limit or may be disallowing its use and export. In some jurisdictions wherever the utilization of cryptography is legal, laws allow investigators to compel the revealing of cryptography keys for documents relevant to associate investigation. Cryptography additionally plays a serious role in digital rights management and violation of digital media [4].

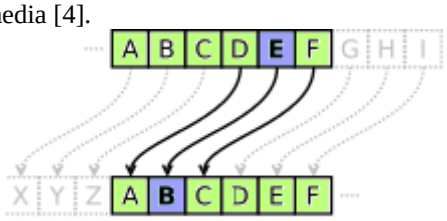

Figure-1 An example, which shows the letters in alphabet are shifted 3 in one direction for encrypt and 3 in the other direction for decrypt [1].

The cryptanalysis of the new mechanical devices tried to be each tough and toilsome. Within the UK, cryptological efforts at Bletchley Park throughout WWII spurred the event of a lot of economical suggests that for polishing off reiterative tasks. This culminated within the development of the Colossus, the world's 1st absolutely electronic, digital, programmable computer, that power-assisted within the decipherment of ciphers generated by the German Army's animal scientist SZ40/42 machine.

Just as the event of digital computers and natural philosophy helped in cryptography, it created potential way more advanced ciphers. What is more, computers allowed for the secret writing of any reasonably knowledge expressible in any binary format, in contrast to classical ciphers that solely encrypted written communication texts; this was new and vital. The computer use has therefore supplanted linguistic cryptography, each for cipher style and cryptography. Several computer ciphers are often characterized by their operation on binary bit sequences i.e., sometimes in teams or blocks, in contrast to classical and mechanical schemes, that usually manipulate ancient characters i.e., letters and digits directly. However, computers have conjointly power-assisted cryptography that has remunerated to some extent for accumulated cipher complexness. Yet, smart fashionable ciphers have stayed previous cryptanalysis; it's usually the case that use of a top quality cipher is incredibly economical i.e., quick and requiring few resources, like memory or central processor capability, whereas breaking it needs a trial several orders of magnitude larger, and immensely

larger than that needed for any classical cipher, creating cryptography thus inefficient and impractical on be effectively not possible.

Extensive open educational analysis into cryptography is comparatively recent; it began solely within the mid-1970s. In recent times, IBM personnel designed the formula that became the Federal i.e., US encryption Standard; Whitfield Diffie and Martin Lillian Hellman printed their key agreement formula; and also the RSA algorithm was printed in Martin Gardner's scientific yank column. Since then, cryptography has become a wide used tool in communications, computer networks, and computer security usually. Some trendy scientific discipline techniques will solely keep their keys secret if bound mathematical issues are uncontrollable, like the number resolution or the distinct index issues, thus there are deep connections with abstract arithmetic. There are only a few cryptosystems that area unit evidenced to be flatly secure. The one-time pad is one. There are many vital ones that are evidenced secure below bound unproved assumptions. As an example, the impracticability of factorization extraordinarily giant integers is that the basis for basic cognitive process that RSA is secure, and a few different systems, however even there, the proof is sometimes lost attributable to sensible concerns. There are systems like RSA, like one by archangel O. Rabin that's demonstrably secure provided factorization a=bc is not possible, however the a lot of sensible system RSA has ne'er been evidenced secure during this sense. The distinct index drawback is that the basis for basic cognitive process another cryptosystems are secure, and again, there are connected, less sensible systems that are demonstrably secure relative to the distinct log drawback [1].

As well as being attentive to cryptographical history, cryptographical algorithmic rule and system designers should conjointly sanely take into account probable future developments whereas performing on their styles. For example, continuous enhancements in computer process power have accumulated the scope of brute-force attacks, therefore once specifying key lengths, the desired key lengths are equally advancing. The potential effects of quantum computing are already being thought of by some cryptographical system designers; the declared state of little implementations of those machines is also creating the necessity for this preventative caution rather quite just speculative [1].

Essentially, before the first twentieth century, cryptography was in the main involved with linguistic and authorship patterns. Since then the stress has shifted, and cryptography currently makes intensive use of arithmetic, as well as aspects of data theory, process quality, statistics, combinatorics, abstract pure mathematics, range theory, and finite arithmetic usually. Cryptography is additionally a branch of engineering, however algorithm uncommon one since it deals with active, intelligent, and malevolent opposition; different kinds of engineering e.g., civil or chemical engineering, would like deal solely with neutral natural forces. There's conjointly active analysis examining the link between cryptographical issues and physics [5].

II. MULTICAST SOURCE DISCOVERY PROTOCOL (MSDP)

Multicast supply Discovery Protocol i.e., MSDP may be a Protocol Independent Multicast i.e., PIM family multicast routing protocol outlined by Experimental RFC 3618. MSDP interconnects multiple IPv4 PIM Sparse-Mode i.e., PIM-SM domains that allow PIM-SM to possess Rendezvous purpose redundancy and inter-domain multicasting RFC 4611.

MSDP uses protocol as its transport protocol. Every multicast tree must have its own RP. All of the RP's are peers directly or through different MSDP peers. Messages contain supply of knowledge, cluster Address the data sends to (S, G). If RP on its own domain receives a message it determines if there are cluster members on this domain curious about a multicast. If somebody is interested it triggers be part of towards the data source into the supply domain within the manner of (S, G). During a peering relationship, one MSDP peer listens for brand new protocol connections on the well-known port 639. MSDP is that the protocol for IPv4 and IPv6 Multicast [6].

When RP during a PIM-SM domain 1st learns of a replacement sender, e.g., via PIM register messages, it constructs a "Source-Active" (SA) message and sends it to its MSDP peers. All RPs, that shall originate or receive SA messages, should establish MSDP peering with different RPs, either directly or via intermediate MSDP peer. The SA message contains the subsequent fields like to supply address of the data source, to cluster address the info supply sends to, informatics address of the RP etc. Note that a RP that may not a DR on a shared network mustn't originate SA's for directly connected sources thereon shared network; it ought to solely originate in response to receiving Register messages from the DR [7].

Each MSDP peer receives and forwards the message far away from the RP address during a "peer-RPF flooding" manner. The notion of peer-RPF flooding is with relevancy forwarding SA messages. The Multicast RPF routing info Base (MRIB) is examined to see that peer towards the originating RP of the SA message is chosen. Such a peer is termed AN "RPF peer". If the MSDP peer receives the SA from a non-RPF peer towards the originating RP, it'll drop the message. Otherwise, it forwards the message to all or any its MSDP peers except the one from that it received the SA message.

When a MSDP peer that is additionally a RP for its own domain receives a new SA message, it determines if there are any cluster members among the domain curious about any cluster delineate by an (Source, Group), or (S, G) entry among the SA message. That is, the RP checks for a (*, G) entry with a non-empty outgoing interface list; this suggests that some system within the domain is curious about the cluster. During this case, the RP triggers a (S, G) be part of event towards the data source as if a Prune message was received addressed to the RP itself. This sets up a branch of the source-tree to the present domain. Ulterior information packets make the RP via this branch, and are forwarded down the shared-tree within the domain. If leaf routers like better to be part of the therefore urce-tree they need the choice to try and do so in step with existing PIM-SM conventions. Finally, if a RP during a domain receives a PIM be part of message for a replacement cluster G, the RP ought to trigger a (S, G) be part of event for every active (S, G) for that cluster in its SA cache. This procedure has been dear named flood-and-join as a result of if any RP isn't

curious about the cluster; they'll ignore the SA message. Otherwise, they are part of a distribution tree [7].

A digital watermark [8] may be a quite marker covertly embedded in a very noise-tolerant signal like audio, video or image information. It's usually accustomed determine possession of the copyright of such signal. "Watermarking" is that the method of concealing digital info during a carrier signal; the hidden info ought to, however ought not to, contain a relevancy the carrier signal. Digital watermarks is also accustomed verify the credibility or integrity of the carrier signal or to indicate the identity of its house owners. It's conspicuously used for tracing copyright infringements and for folding money authentication.

Figure-2 The picture of a watermark overlay on an image

Like ancient physical watermarks, digital watermarks are usually solely perceptible below bound conditions, i.e. when mistreatment some rule. If a digital watermark distorts the carrier signal in an exceedingly manner that it becomes simply perceivable, it should be thought of less effective looking on its purpose. Ancient watermarks are also applied to visible media i.e., pictures or video, whereas in digital watermarking, the signal is also audio, pictures, video, texts or 3D models. A symbol might carry many totally different watermarks at an equivalent time. In contrast to data that's additional to the carrier signal, a digital watermark doesn't modification the scale of the carrier signal.

The required properties of a digital watermark rely upon the employment case within which it's applied. For marking media files with copyright data, a digital watermark should be rather strong against modifications which will be applied to the carrier signal. Instead, if integrity should be ensured, a fragile watermark would be applied.

The information to be embedded in an exceedingly signal is termed a digital watermark, though in some contexts the phrase digital watermark means that the distinction between the watermarked signal and therefore the cowl signal. The signal wherever the watermark is to be embedded is termed the host signal. A watermarking system is typically divided into 3 distinct steps, embedding, attack, and detection. In embedding, algorithm accepts the host and therefore the information to be embedded, and produces a watermarked signal.

Then the watermarked digital signal is transmitted or keeps, sometimes transmitted to a different person. If this person makes a modification, this is often referred to as algorithm attack. Whereas the modification might not be malicious, the term attack arises from copyright protection application, wherever third parties might arrange to take away the digital watermark through modification. There are several doable modifications, as an example, loss compression of the information, cropping a picture or video or deliberately adding noise.

Detection i.e., extraction is algorithm rule that is applied to the attacked signal to try to extract the watermark from it. If the signal was unmodified throughout transmission, then the watermark still is gift and it should be extracted. In strong digital watermarking applications, the extraction rule ought to be ready to manufacture the watermark properly, even though the modifications were robust. In fragile digital watermarking, the extraction rule ought to fail if any modification is formed to the signal. The method of digital watermark life-cycle phases is shown in figure-3.

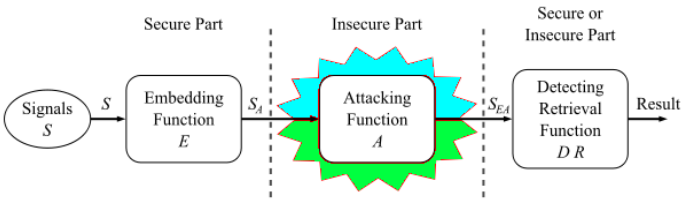

Figure-3 The process of life-cycle phases of digital watermarking [8]

III. MATHEMATICAL ALGORITHM

The algorithm given by Yahya AL-Nabhani et al., (2015) [9] for embedding the watermark is as follows:

Step 1: A grayscale cowl image with constituent dimensions of 512x512 is 1st hand-picked.

Step 2: A grayscale watermark image with constituent dimensions of 64x64 is employed as a watermark. The watermark image is then reborn into the binary format.

Step 3: 3 levels of rippling decomposition area unit performed for the first cowl image with the employment of the filter. The DWT processes the image by rending it into four non-overlapping multi-resolution sub-bands: LL, LH, HL, and HH. The sub-bands interstitial cell-stimulating hormone, HL, and HH represent the fine-scale of DWT coefficients, whereas the sub-band LL represents the coarse-scale of DWT coefficients. For every consecutive level of rippling decomposition, the LL sub-band of the previous level is employed as input. Finally, we have a tendency to acquire four sub-bands of 3 levels, namely, LL3 (cA3), LH3 (cH3), HH3 (cD3), and HL3 (cV3), every of that is 64x64 pixels. Moreover, the first image is reconstructed from these DWT coefficients. This reconstruction method is named the inverse DWT (IDWT).

Step 4: The 3 rippling sub-band coefficients (cH3, cD3, and cV3) with constituent dimensions of 64x64 are split into non-overlapping tiny blocks with constituent dimensions of 4x4. This technique produces 16x16 blocks for every constant.

In this study, the fascinating options of rippling rework area unit incorporated to realize the most advantages. Most of the energy of a picture is targeted within the low-frequency constant block LLi. Meanwhile, embedding the watermark within the high-frequency constant blocks HHi (cH3, cD3, cV3), that represent the fine-scale of DWT coefficients, renders the watermark unperceivable to the human eye.

Step 5: The watermark binary image with constituent dimensions of 64x64 is split into tiny, non-overlapping blocks with constituent dimensions of 4x2, therefore

manufacturing 16x32 blocks. These blocks are then embedded into the chosen rippling constant blocks. However, the watermark is embedded block by block, instead of being reborn into a vector that facilitates embedding. This method includes a discount within the loop iteration and time interval. This step conjointly allows easy management and follows the flow of the embedded information.

Step 6: Watermark blocks area unit embedded into the cH3, cD3, and cV3 blocks by the subsequent embedding equation given as: $I'(i, j)=I(i, j)+\alpha(w-1)$

Where I (i, j) is that the original constant of the chosen block, I′(i, j) is that the watermarked constant akin toI(i, j), w is that the watermark bit, and α is that the embedding strength constant that controls the watermarking strength. The worth of α directly influences embedding effectiveness and is chosen by experimentation.

To ensure high watermarking quality, the watermark blocks are embedded within the 3 rippling coefficients (cH3, cD3, and cV3) consecutive, as follows:

1. The first 1/4 of the watermark pixel values are embedded into cH3.
2. The second 1/4 of the watermark pixel values are embedded into cD3.
3. The remaining 1/2 of the watermark pixel values is embedded into cV3.

Step 7: Inverse decomposition rippling rework is performed on every constant to get the watermarked image.

IV. RELATED RESEARCHES

F. A. P. Petitcolas, (1999) [10] represented variety of attacks on data concealment systems, that between them demolish most of this contenders within the copyright marking business. They represented a tool, StirMark, that breaks several of them by adding sub-perceptual distortion; and that they have represented a custom attack on echo concealment.

Ahmed A. Radwan et al., (2011) [11] have said that the enhancements in net technologies and growing requests on on-line multimedia system businesses have created digital copyrighting as a big challenge for businesses that are connected with on-line content distribution via various business models as well as pay per view, subscription, trading, etc. Copyright protection and therefore the proof for rightful possession are major problems connected with the distribution of any digital pictures. Digital watermarking is one amongst the advised solutions for copyright protection of multimedia system knowledge. According to them the method is best than Digital Signatures and alternative strategies as a result of it doesn't rise overhead. In their paper, there is a brand new watermarking technique that supported spatial domain image steganography technique known as MSLDIP i.e., Modified Substitute Last Digit in Pixel is planned. The most goal of this technique is to cover the watermark within the pixels of digital image in such a way that the human sensory system isn't able to distinguish between the duvet image and therefore the watermarked image.

D. Biswas et al., (2011) [12] have showed that in case of direct watermarking, if the secret image contains a higher concentration of white pixels, then LSB-MSB offers higher PSNR results. However if a lot of pixels are of darker colors, LSB-LSB offers higher results.

Preeti Gupta et al., (2012) [13] have said that Digital Watermarking describes ways and technologies that hide data, for instance variety or text, in digital media, like pictures, video or audio. The embedding takes place by manipulating the content of the digital knowledge, which implies the information isn't embedded within the frame round the data.

Deepshikha Chopra et al., (2012) [14] have declared that the increasing quantity of digital exchangeable knowledge generates new data security desires. Transmission documents and specifically pictures also are affected. Users expect that sturdy solutions can guarantee copyright protection and conjointly guarantee the legitimacy of transmission documents. Within the current state of analysis, it's tough to affirm that watermarking approach looks best suited to make sure algorithm integrity service tailored to photographs and a lot of general thanks to transmission documents. The tool used for the execution of this formula was “Matlab”. The aim of the program is to exchange the LSB of the bottom image with the MSB of the watermark.

S. A. Baker et al., (2013) [15] have projected a replacement image steganographic technique capable of manufacturing a secret-embedded image that's entirely indistinguishable from the first image by the human eye within mobile through Bluetooth. The projected methodology performs permutation XOR operation on secret message image with the bit extracted from constituent of canopy image and eventually LSB replacement with the image pixels. This targeted on increasing the protection by creating use of pseudo-randomized key and conjointly applicable to paint level pictures.

S. Deepa et al., (2013) [16] have said that in these days steganography is usually used on computers with digital information being the carriers and networks being the high speed delivery channels. The less complicated systems will be utilized in such the simplest way that they create life more durable for the steganalyst, just by embedding shorter messages. Short messages produce a shorter bit-stream that successively needs less bit-flip to introduce. With fewer modifications created to a picture, it's a lot of more durable to identify a distinction between the stegogramme and a clean version of a similar image. It’s still extremely possible that a whole steganographic system would possibly use science measures as a safety-net to safeguard the content of the message within the event that the steganography is broken.

Monika Patel et al., (2013) [17] have introduced the classification of digital watermarking techniques. These techniques are classified into many classes relying upon the domain during which the hidden information is inserted and also the demand of which the hidden information is to be extracted. They have additionally conferred frequency domain methodology named as DWT based mostly watermarking technique with embedding and extraction method. Their experiment shows that frequency domains are usually higher candidates for watermarking than spatial domain, for each reasons of lustiness likewise as visual impact. The result indicates wave coded image may be a multi-resolution description of image. In DWT a picture will be shown at completely different levels of resolution and might be consecutive processed from low resolution to high resolution by ever-changing the scaling issue. In future this digital watermarking technique is going to been forced for

the digital information like text, 3-Dmeshes, face animation parameters, video and audio.

Abdelmgeid A. Ali et al., (2014) [18] have shown that the Digital watermarking is one in all the steered solutions for copyright protection of multimedia system knowledge. This system is healthier than Digital Signatures and alternative ways as a result of it doesn't rise overhead. In their paper a brand new watermarking methodology was introduced that supported abstraction domain image steganography methodology known as MSLDIP i.e., Modified Substitute Last Digit in Pixel is projected. The most goal of this methodology is to cover the watermark within the pixels of digital image in such a fashion that the human sensory system isn't ready to distinguish between the quilt image and therefore the watermarked image.

Krishna Kumar et al., (2014) [19] have cleared that the Cryptography in digital watermarking is that the current space of analysis wherever ton of scope exists. Presently cryptographical technique in digital watermarking is getting used by many countries for on the QT transfer of hand written documents, monetary documents, text pictures, net pick etc. There are numerous innovative concepts and extensions exist for the fundamental cryptographical technique introduced until currently.

Z. K. Abdalrdha et al., (2015) [20] have used the steganography methodology that supported Least important Bit (LSB). The techniques that are optimized by XOR methodology, that will increase the safety of the text before being sent across the medium by concealment messages with in a picture, and will increase the confidentiality by victimization error correction code algorithmic rule to produce cipher text which will be recovered. It had been designed for color pictures that were sent by Viber, WhatsApp, and E-mail programs, thus it'll be tough by unauthorized folks to extract the first messages. The projected approach is tested victimization differing kinds of mobile phones.

V. CONCLUSION

Thus last that Digital Watermarking has importance in securing digital contents from unauthorized user. SLDIP and MSLDIP techniques are enforced for this purpose, and from results conclude that the visual quality of the image does not modification considerably, on the opposite hand this algorithmic rule is a lot of sturdy than LSB technique, as a result of in LSB technique some attackers will probably zero out many least important little bit of pixels of the image and therefore clear the watermark. This method has exaggerated the capability of embedding watermark. Within the future a lot of security is thought of to stop unauthorized users from police investigation the watermark from the image by exploitation coding algorithmic rule and a lot of strength can thought of by exploitation frequency domain.

VI. REFERENCES

[1] Cryptography From Wikipedia, the free encyclopedia, 28th March, 2017. https://en.wikipedia.org/wiki/Cryptography.

[2] R. L. Rivest, “Cryptography,” In J. Van Leeuwe, Handbook of Theoretical Computer Science, 1, 1990, Elsevier.

[3] M. Bellare and P. Rogaway, “Introduction to Modern Cryptography,” p. 10.

[4] A. J. Menezes, P. C.Van Oorschot and S. A. Vanstone, “Handbook of Applied Cryptography,” ISBN 0-8493-8523-7. Archived from the original on 7 March 2005.

[5] N. Biggs, “Codes: An introduction to Information Communication and Cryptography,” Springer, 2008, p. 171.

[6] Multicast Source Discovery Protocol From Wikipedia, the free encyclopedia, 6 September 2016. https://en.wikipedia.org/wiki/Multicast_Source_Discovery_Protocol.

[7] Fenner & Meyer, Experimental analysis on MSDP RFC 3618, October 2003, pp. 3.

[8] Digital watermarking From Wikipedia, the free encyclopedia, 17th March 2017. https://en.wikipedia.org/wiki/Digital_watermarking.

[9] Y. AL-Nabhani , H. A. Jalab, A. Wahid and R. Md Noor, “Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network” Journal of King Saud University - Computer and Information Sciences,Volume 27, Issue 4, October 2015, pp. 393- 40. http://dx.doi.org/10.1016/j.jksuci.2015.02.002

[10] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, “Information Hiding - A Survey,” proceedings of the IEEE, Special Issue on Protection of Multimedia Content, vol. 87(7), pp.1062 - 1078, July 1999.

[11] A. A. Radwan, A. Swilem and Al-Hussien Seddik, “A High Capacity SLDIP method,” ICICIS, July 2011.

[12] D. Biswas, S. Biswas, P. P. Sarkar, D. Sarkar, S. Banerjee and A. Pal, “COMPARISON AND ANALYSIS OF WATERMARKING ALGORITHMS IN COLOR IMAGES – IMAGE SECURITY PARADIGM,” International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, June 2011. DOI: 10.5121/ijcsit.2011.3303 33.

[13] P. Gupta, “Cryptography based digital image watermarking algorithm to increase security of watermark data”, International Journal of Scientific & Engineering Research,Volume 3, Issue 9 (September 2012) ISSN 2229-5518.

[14] D. Chopra, P. Gupta, G. Sanjay and A. Gupta, “LSB based digital image watermarking for gray scale image,” IOSRJCE, October 2012.

[15] S. A. Baker and A. S. Nori, “Steganography in Mobile Phone over Bluetooth,” International Journal of Information Technology and Business Management (JITBM),Volume 16, Number 1, Pages 111- 117, 29 August 2013.

[16] S. Deepa and R. Umarani, "A Study on Digital Image Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, InternationalJournal of Advanced Research in Computer Science and Software Engineering, Volume 3,Issue 1, January 2013.

[17] M. Patel, P. S. Sajja and J. Patel, “Enhancement of DWT based Watermarking Technique for Images,” International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 12, December 2013, pp. 4750-4756.

[18] A. A. Ali, A. Radwan, and A. H. Ismail, “Digital Image Watermarking using MSLDIP (Modified Substitute Last Digit in Pixel),” IJCA, Volume 108, No 7, pp. 30-34, December 2014.

[19] K. Kumar and S. Dwivedi, “Digital Watermarking using Asymmetric Key Cryptography and Spatial Domain Technique,” IJARCSMS, Volume 2, Issue 8, August 2014.

[20] Z. K. Abdalrdha and M. T. Ajjah, “Modifying Steganography in Android Mobile Image Based onECC Algorithm,” Al-Mustansiriyah Journal of Science Vol. 26, No 1, 2015, pp. 77-83.