Copyright Protection Protocols For Copyright Protection Issues

YAMUNA GOVINDHARAJAN and SIVAKUMAR DAKSHINAMURTHI
Department of Electrical and Electronics Engineering
Annamalai University
Chidambaram
INDIA
yamunaphd@yahoo.com

Abstract: - With the pervasiveness of internet, businesses online have become ubiquitous. The proposed concept is a solution with a specific focus on preventing disputes that comes out of ownership claims through buying and selling digital documents. The concept proposed offers a dependable watermarking method that can help authenticate sellers and buyers of digital documents. The important issues of copyright protection such as buyer-owner identification, copyright infringement, and ownership verification are addressed. Embedding the owners' and buyers' identities through watermarks and provisions for revealing the same as proof to substantiate the ownership rights of buyer over the digital document, will serve as a solution for issues arising out of buyer owner identification. To solve copyright infringement issues, the concept offers necessities that can help the owner to identify the buyer, from whom the illegal copies of the documents originated. The provisions to identify the legal owner of the digital document, can settle controversies regarding multiple ownership claims in the court of law. The usage of DCT-SVD based watermarking and public key encryption with hash values fortifies the scheme and makes it a fail-safe method.

Key-Words:- Digital Watermarking, Copyright Protection, Copyright Infringement, Multiple ownership Disputes.

1 Introduction

The rapid growth of multimedia content in digital form has increased the need to develop secure methods for legal distribution of the digital content. Security of digital images has become a great importance with the omnipresence of internet The advent of image processing tools has increased the vulnerability for illicit copying, modifications, and dispersion of digital images. Techniques like digital watermarking are put into practice to prevent unauthorized replication or exploitation of digital images [3], [4], [5], [6]. A digital watermark is a distinguishing piece of information that remains along with the data that it is intended to protect, which is usually very difficult to extract or remove the watermark from the watermarked object [1]. The watermark could be visible or invisible. A visible watermark contains an evident visible message or a company logo indicating the rightful ownership of the image. The invisibly watermarked content appears perceptually identical to the original. A detection algorithm can be used to extract the invisible watermark [2]. Guaranteeing protection against copyright infringements and completely addressing the issues pertaining to contravention, demands much more than mere utilization of watermarking algorithm.

Symmetric and asymmetric schemes of digital watermarking can be deployed for the stated purposes. Embedding and Extraction of watermarks require identical keys in symmetric watermarking schemes and these schemes have become quiet obsolete as they are very much prone to attacks. Usage of symmetric watermarking has inherent susceptibility as the key used for watermarking is the same one to be used for extraction. In asymmetric watermarking, the shortcoming of having similar keys in symmetric schemes is rectified through the application of dissimilar keys for watermarking and detection. The technique proves compatible for catering the requirements in public domain applications, since the key required for deciphering is atypical of the ones used for ciphering, in asymmetric schemes. Despite these features, application of asymmetric watermarking requires considerable reassessment [20].

Incorporation of a secure protocol with a watermarking algorithm proves inevitable to formulate a secure watermarking scheme [21], [22]. Interactive buyer/owner protocols proposed [15] blinds the owner from knowing the exact watermark

references inserted for that particular buyer. This process can in turn prevent the owner from reusing the buyer's references while dealing with other customers. Proving to a third party, the buyer from whom the unauthorized copies originated, becomes feasible through this protocol. To address the issues related to copyright protection and buyer/owner identification we integrated cryptographic protocols with some of the existing watermarking techniques and developed a new strategy. This process apart from accumulating the robustness and reliability of the constituent techniques exploits them to the optimal level and configure a powerful solution to the stated problems.

To further enunciate our intent, we present few situations where controversies usually pop out. Presume a owner sells a watermarked image to a buyer. Subsequently, the buyer begins selling the watermarked image without being authorized to do so. Is there an option to prevent the buyer from selling copies of document he has purchased from an authorized owner, without having the rights to involve in distribution of the same? How can the legal owner distinguish himself as the actual owner, while the watermarked document contains the identities of both the owner and the buyer? What if the buyer manages to obliterate the legal owner's watermark from the image, and how can the genuine owner assert his ownership in this case. Another sticky situation would be that an owner sells a watermarked document D_w to a buyer, consequently the extraction of watermark from the D_w would testify that the buyer has in fact procured the watermarked document from the owner. How such watermarks, which reveal the identities of the buyers and owners, can be designed leaving no room for repudiation?.

The proposed concept extracts the synergistic power of cryptographic techniques with watermarking. The processes reassure substantial improvement in terms of security at the same time helps integrating the identities of the owner and buyer. Therefore the watermarked images will carry the identities of the buyer and owner acquired from a Certification Authority and is bound to the respective parties through a Registration Authority. These references are indubitably unique and beyond any controversies pertaining to possession of similar identities. The proposed concept addresses some of the very serious issues of copyright protection that includes verification of ownership, buyer/owner identification and copyright infringements. The steps in the process contribute to the identification of the legal owner of the watermarked image through categorical proof and help settle issues concerned to multiple ownership claims. The copyright infringement disputes can be elucidated using the proposed concept through the specifications that help recognition of the buyer from whom the illegal copies of the watermarked images originated. Buyer/owner identification is performed through embedding references regarding the identities of the buyer and owner. This information can be successfully revealed at the buyer's end from the watermarked image.

The paper is organized as follows. Section 2 discusses the related work in watermarking and copyright protection protocols. In Section 3, we present the copyright protocols along with the watermark embedding and extraction techniques. Section 4 presents the attacks and section 5 concludes the paper.

2 Related Work

Jeffrey A Bloom et al. [11] describe the copy protection system currently under consideration for DVD and they discuss some proposed solutions and some of the implementation issues that are being addressed.

Ingemar J.Cox et al. [12] present a secure algorithm (tamper-resistent) algorithm for watermarking images and a methodology for digital watermarking that may be generalized to audio, video and multimedia data.

T. Furon et al. [13] presents an asymmetric watermarking method as an alternative to classical Direct Sequence Spread Spectrum and Watermarking Costa Schemes techniques and their method proof that the Kerckhoffs principle can be stated in the copy protection framework.

Joachim J. Eggers et al. [14] have proposed the new approaches are significantly less complex than the public watermark detection principle that works without explicit reference to the embedded signal.

Nasir Memon et al. [15] proposes an interactive buyer-seller protocol for invisible watermarking in which the seller does not get to know the exact watermarked copy that the buyer receives and their approach prevents the buyer from claiming that an unauthorized copy may have originated from the seller.

R.L. Rivest et al. [16] developed an encryption method with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key.

Neil F.Jhonson et al. [17] propose alternative methods for image recognition based on the concept of identification marks (id-marks of fingerprints).

Joshua R. Smith et al. [18] introduce new information hiding schemes whose parameters can easily be adjusted to trade off capacity, imperceptibility, and robustness as required in the application by use concepts from communication theory to characterize information hiding schemes

Jian Zhao et al. [19] discussed a set of novel steganographic methods to secretly embed robust labels into image data for identifying image copyright holder and original distributor in digital networked environment.

3 Copyright Protection Protocols

The proposed concept is a solution with a specific focus on preventing disputes that comes out of ownership claims through buying and selling digital documents. The problem necessitates a fool-proof mechanism to substantiate the ownership of document before it is sold and a similar structure to attest authentic buyers. The concept takes into consideration these issues and proposes a solution to overcome controversies if any. Hence the requirement can be categorized as

- Need to establish ownership identities and
- Prevention of copyright infringements
- Need to resolve the owner – Buyer claims

Our proposed protocols are discussed as follows

1) Ownership Identity Watermarking Protocol.
2) Transaction Identity Watermarking Protocol.
3) Transaction Identity Protocol.
4) Copyright Infringement Protocol

3.1 Ownership Identity Watermarking Protocol

The requirement to establish ownership identity should be armored enough to proclaim the possession of the ownership under any circumstances. To trace illegal copies of the original data, a unique watermark is needed for transaction between each buyer. The protocol fulfils this requirement through imprinting a watermark over the document. The protocol proceeds as follows.

1. The owner hashes the original image I to get the hashed image $H(I)$.
2. Then the owner hashes the buyer's public key and combines it with $H(I)$ to get the owners identity watermark W_{OI} which is a unique watermark for the transaction with the corresponding buyer.
$$W_{OI} = H(I) + H(K_B^{Pub}) \quad (1)$$
3. Then the owner encrypts the owner's identity watermark W_{OI} using his public key K_O^{Pub}.
$$E_{K_O^{Pub}}(W_{OI}) = Enc(W_{OI})_{K_O^{Pub}} \quad (2)$$
4. The owner sends the encrypted watermark $E_{K_O^{Pub}}(W_{OI})$ along with his identity and public key K_O^{Pub} to the certification authority (CA) for a digital signature.
5. The CA verifies the identity of the owner and then hashes the encrypted watermark, public key and timestamp to get $H(E_{K_O^{Pub}}(W_{OI}), K_O^{Pub}, T_1)$ where T_1 is the time stamp which is used to solve multiple ownership disputes.
6. A tuple T_{CA} is formed by combining the above hash information and timestamp T_1. Then the tuple T_{CA} is hashed to get $H(T_{CA})$.
$$T_{CA} = \{H(E_{K_O^{pub}}(W_{OI}), K_O^{Pub}, T_1), T_1\} \quad (3)$$
7. A digital signature DS_{CA} is obtained by encrypting $H(T_{CA})$ with CA's private key K_{CA}^{Pri} and then with owner's public key.
$$DS_{CA}(T_{CA}) = E_{K_O^{pub}}(K_{CA}^{Pri}(H(T_{CA}))) \quad (4)$$
8. The CA then sends the certificate Cer_{ow} to the owner.
$$Cer_{ow} = \{T_{CA,}, DS_{CA}(T_{CA})\} \quad (5)$$
9. The owner verifies Cer_{ow} by first decrypting it with CA's public key K_{CA}^{Pub} and then with his private key K_O^{Pri} to get $H(T_{CA})$. Then the owner hashes T_{CA} to get $H_1(T_{CA})$. *If* $H_1(T_{CA}) = H(T_{CA})$, it will be verified that the Cer_{ow} has been generated by the CA and that it has not been tampered. Then the owner keeps this certificate as a proof of his copyright to solve ownership disputes.
10. The owner then embeds the encrypted watermark $E_{K_O^{Pub}}(W_{OI})$ in to the original image to get ownership watermarked image I_{OI}.
$$I_{OI} = I \lhd E_{K_O^{pub}}(W_{OI}) \quad (6)$$

Where $\lhd$ denotes the embedding process.

The hash value derived out of the document is irreversible i.e.; the document through which the

hash value is obtained cannot be regenerated from the hash value itself. This hash value is reliably unique and the chances of having identical hash values from two different documents are negligibly thin. Unwarrantedly, the prospect of creating a similar watermark is impractical. Furthermore encrypting this hash value with the owner's public key reinforces the resilience of the watermark. Even if a brute force attack is attempted to derive a hash value, decryption poses a major challenge due to this aspect.

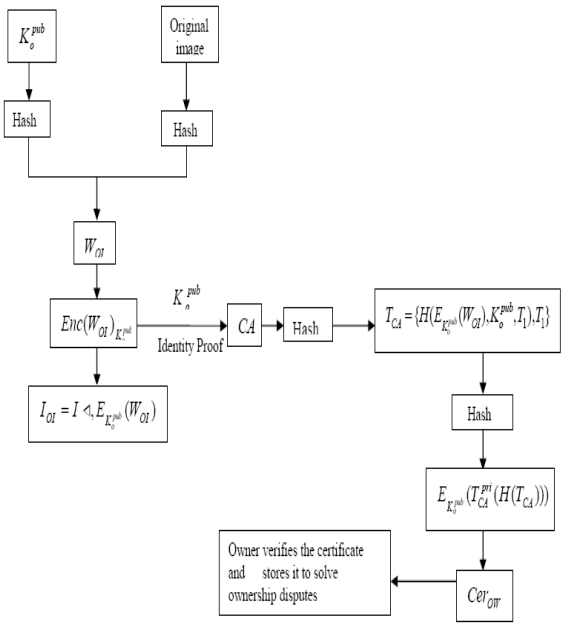

Fig 1 : Block Diagram for Ownership Identity Watermarking Protocol

3.1.1 Ownership Identity Watermark Embedding

The technique chosen to embed the ownership identity watermark should be robust, due to the reasons mentioned hereunder. Ownership identity watermark is the only means through which a genuine owner can prove his ownership. The watermark should be robust enough to withstand distortions to a certain degree and should be foolproof to be identified and altered by unauthorized people. The primary intent of watermark is to protect copyright infringements and thereby preventing ownership dispute claims. This ownership identity watermark embedded should also be resilient against possible misrepresentations that can happen in the course of imprinting transaction identity watermark –performed to embed buyer identities.

According to Mintzer and Braudaway [7] the magnitude of robustness requirements of individual watermarks vary in multiple watermarking in accordance to the purposes they serve. The order of embedding watermarks too plays a significant role. Moreover it is suggested, the watermarks that serve the purpose of ownership identification should be embedded first and the delicate watermarks can be given least priority and the moderately robust watermarks can be integrated in between. This process guarantees the most robust watermark will able to endure all consequent watermark insertions.

The ownership identity watermark –performed for embedding ownership identity, requires a higher degree of robustness than the transaction identity watermark –performed to embed buyer identities

The fail-safe aspect of the proposed technique relies on the possession of the original image. Ownership identity watermarking technique uses a non-blind watermarking method.. This method ensures that without using the Original Image, the Watermark Information from the Watermarked image cannot be extracted. The method also guarantees that anyone other than the owner of the Original Image cannot claim the ownership once the image is watermarked. We have used the DCT-SVD domain image watermarking proposed by Alexander Sverdlov et al [8] which is a non-blind watermarking scheme. This technique is robust against a number of attacks as discussed in [8].

This technique is based on DCT and SVD. After applying the DCT to the cover image, it maps the DCT coefficients in a zig-zag order into four quadrants, and apply the SVD to each quadrant. These four quadrants represent frequency bands from the lowest to the highest. The singular values in each quadrant are then modified by the singular values of the DCT-transformed visual watermark.

3.1.2 Ownership Identity Watermark Extraction

The private-watermark extraction is nonblind and requires the original image I. The technique to extract the watermark from the watermarked image is described by the following steps [8].

- Apply the DCT to the whole watermarked.
- Using the zig-zag sequence, map the DCT coefficients into 4 Quadrants.
- Apply SVD to each quadrant.
- Extract the singular values from each quadrant
- Construct the DCT coefficients of the four visual watermarks using the singular vectors.
- Apply the inverse DCT to each set to construct the four visual watermarks.

3.2 Transaction Identity Watermarking Protocl

This protocol takes care of attesting the buyer information into the purchased digital document. The information is embedded as another watermark to serve as a testimony to authenticate the buyer. This watermark apart from being robust will render provisions to portray its content when unveiled for corroboration of the authenticity of the buyer. Even in cases where the buyer resells the same without being authorized to do so, the protocol helps to trace out such activities. This process also ensures that no buyers without the required privileges can involve in distribution of digital documents since the buyers' identity is entrenched too.

1. The owner combines his public key K_O^{Pub} and the public key of the buyer K_b^{Pub} to form the message Ms.
2. Then the owner hashes the message Ms to get the hashed message bits $H(Ms)$.
3. Then a Transaction Identity watermark W_{TI} and Transaction Identity key K_{TI} is generated from the hashed message bits Ms as described in section 3.2.1.
4. The owner then embeds the Transaction Identity watermark in to the ownership Identity watermarked image I_{OI} to get I_w.

$$I_W = I_{OI} \lhd W_{TI} \quad (7)$$

5. The owner then encrypts the Transaction Identity key K_{TI} using his private key to get CK_{TI}.

$$CK_{TI} = Enc(K_{TI})K_O^{Pri} \quad (8)$$

6. The owner then sends the I_w and CK_{TI} to the buyer.
7. Now the buyer will verify the genuine transaction between him and the owner by first decrypting CK_{TI} using the owner's public key to get K_{TI}. This will ensure that W_{TI} has been embedded by the owner.
8. Then the Transaction Identity watermark is extracted from the I_w as described in section 3.2.2.
9. The buyer repeats steps 1, 2, 3 to derive the W_{TI} and compares with the extracted from I_w.If both are equal the buyer is convinced that the W_{TI} reflect his and the owners genuine identities.
10. Then the buyer sends the following to the owner.

$$DS_B(H(I_W, K_O^{pub})) = E_{K_B^{Pri}}(H(I_w, K_O^{pub})) \quad (9)$$

11. The owner verifies the digital signature $DS_B(H(Iw.K_O^{pub}))$ and stores this digital signature, W_{OI}, K_b^{Pub} as the record of proof for transaction with the buyer.

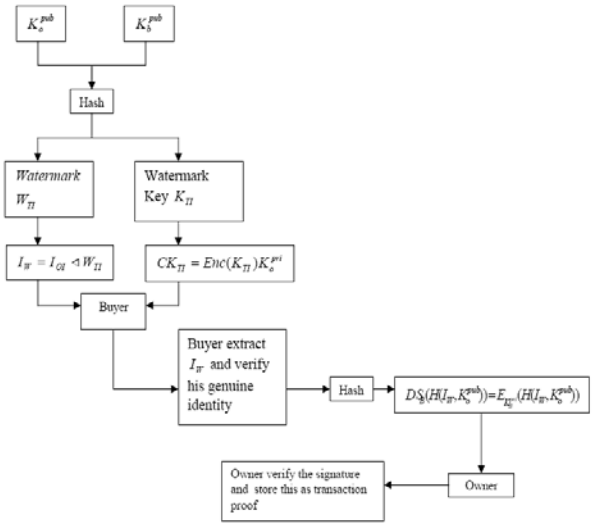

Fig 2 : Block Diagram for Transaction Identity watermarking Protocol

3.2.1 Transaction Identity Watermark Embedding

The purpose of transaction identity watermark embedding is to imprint buyer and owner information into the document. This watermark indicates the transaction between the buyer and the owner and serves as the only means to identify the occurrence of transaction between the buyer and the owner. It also provisions the possibility of extracting the watermark by anyone with the knowledge of transaction identity watermark key. This watermark will reveal identity of the buyer and the seller in case of disputes pertaining to copyright infringements.

Furthermore it can also help serve to identify the buyer from whom the illegal copies of duplicate document originated. Since the watermark information is constructed with the public keys of the buyer and seller which in turn was acquired from a Certificate Authority, the uniqueness of the keys is beyond suspicion. In addition, registering the public keys with a Registration Authority bounds the key to the concerned party and leaves no room for forging the keys. Hence even if some people

duplicate the key either purposely or accidentally the registration of the original user leaves no ground for a legal claim. To watermark the buyer's identity, a hash value is derived from a combination of the public keys of the buyer and the owner. Then a Transaction Identity Watermark and a key is derived from the hash bits.

The technique implemented for embedding Transaction Identity Watermark should be of lesser degree of robustness compared to the one previously applied for imprinting ownership identity. Having a higher degree of robustness for second watermark could distort the first watermark embedded for ownership identity. We have used DWT based technique to embed the transaction identity watermark. The host image is applied haar wavelet transform and the HL , LH subbands are embedded with the watermark data and random value for all the 0 bits. Then inverse haar transform is appliedss to get the watermarked image. The algorithm for watermark embedding is as follows.

1. Two dimensional Haar wavelet transform is applied to the host image to get the four subbands namely HH , LL , HL , LH .
$$I_{HT} = Haar(I) \quad (10)$$
2. From the four subbands, HL and LH subbands are chosen to embed the watermark data The steps to embed the watermark data in to two subbands is given as follows where k controls the strength of the watermark and K_W is the key to embed the watermark..
$$r = rand(K_W) \quad (11)$$
for each watermark date bit
if watermark date bit $= 0$
$$HL += k^* r \quad (12)$$
$$LH += k^* r \quad (13)$$
end
end
3. The original subbands are replaced with the modified subbands and inverse Haar transform is applied to get the watermarked image.
$$\hat{I} = HaarInv(I_{HT}) \quad (14)$$

3.2.2 Transaction Identity Watermark Extraction

The transaction identity watermark is extracted from the watermarked image using the transaction identity key K_{TI} . The watermarked image is applied haar wavelet transform. The random values are again generated and correlated with the HL and LH subbands. Finally the watermark is extracted using the following algorithm.

1. Two dimensional Haar wavelet transform is applied to the watermarked image to get the four subbands.
$$I_{HT} = Haar(\hat{I}) \quad (14)$$
2. Then the watermark is extracted from the two subbands using the following algorithm.
$$r = rand(K_W); \quad (15)$$
for each i *watermark date bit*
$$C_{HL} = Correlation(HL, r) \quad (16)$$
$$C_{LH} = Correlation(LH, r) \quad (17)$$
$$C[i] = (C_{HL} + C_{LH})/2 \quad (18)$$
end
for each i *watermark date bit*
if $(C[i] > mean(C))$
$$W(i) = 0 \quad (19)$$
else
$$W(i) = 1 \quad (20)$$
end
end

3.3 Transaction Identity Protocol

To illustrate how this protocol works; let us assume, the owner made a transaction with a buyer to sell a digital document. Now the buyer can use this protocol to corroborate that he is a genuine buyer of the watermarked document from the owner. To substantiate the protocol demands the possession of the Watermark I_W , Watermark Key CK_{TI} obtained from the owner, in addition to the public keys of the buyer and the owner. The protocol proceeds as follows.

1. Decrypt CK_{TI} using the owner's public key to get K_{TI} .
2. Then the Transaction Identity watermark is extracted from the I_W using K_{TI} as described in section 3.2.2.
3. Repeat the steps 1, 2, 3 of the Transaction Identity Watermarking protocol to derive the W_{TI} and compares it with the extracted watermark from I_W .
4. If bit wise comparison is success or equal any one can trust or verify the transaction has occurred from the corresponding owner and the buyer

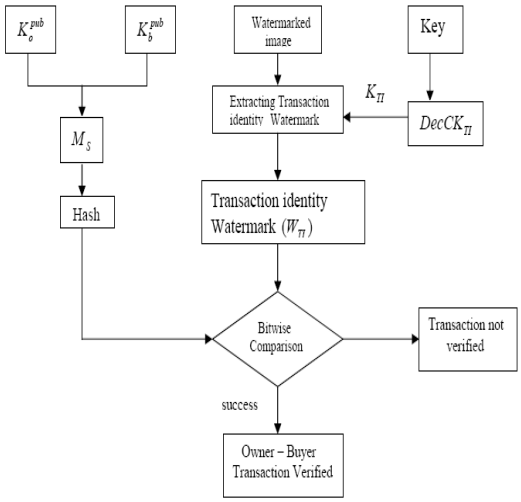

Fig 3: Block Diagram for Transaction Identity Protocol

3.4 Copyright Infringement Protocol

This protocol is meant to solve the issues like when the owner finds an illegal copy of data with an illegal buyer which the owner has not actually issued. The Owner has to prove the illegality in the court and the illegal owner who has actually issued or from which source the illegal buyer has stolen it. We initially follow the same steps discussed in the "Transaction Identity Protocol" to claim himself as the original owner and the buyer who has issued it or from whom it was stolen. The protocol proceeds as follows.

1. Decrypt CK_{TI} using the owner's public key to get K_{TI}.
2. Then the Transaction Identity watermark is extracted from the I_W using K_{TI} as described in section 3.2.2.
3. Repeat the steps 1, 2, 3 of the Transaction Identity Watermarking protocol to derive the W_{TI} and compares it with the extracted watermark from I_W.
4. If bit wise comparison is success or equal any one can trust or verify the transaction has occurred from the corresponding owner and the buyer

If the strength of the embedded Transaction Watermark is reduced in a way the watermark can not be extracted then we follow the following steps.

The owner will extract the unique watermark W_{OI} with his original image I and decrypt with his private key, K_O^{Pri}. Then he extracts the public key of the buyer to whom he has actually sold the image.

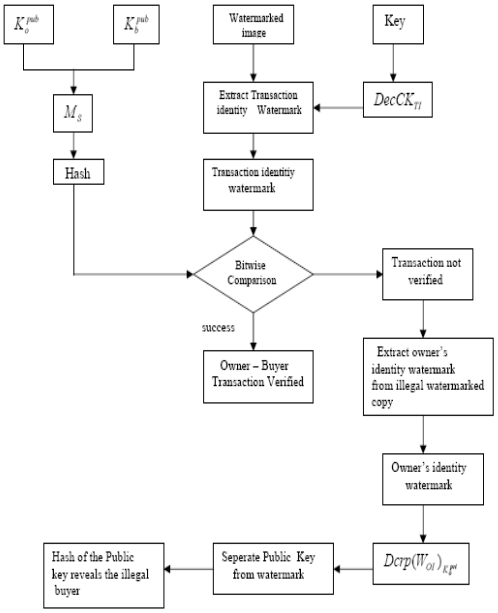

Fig 4: Block diagram for copyright infringement protocol

4. Attacks

Attacks on watermarks may not necessarily remove the watermark, but disable its readability. Image processing and transforms are commonly employed to create and apply watermarks. These same techniques can also be used to disable or overwrite watermarks. Multiple watermarks can be placed in an image and one cannot determine which one is valid. Currently watermark registration service is "first come, first served." Someone other than the rightful owner may attempt to register a copyright first. In this section, we discuss problems that arise in case of multiple ownership claims over a watermarked image. In particular, we illustrate the following three attacks and show how our proposed scheme can resist such attacks:

(A) Ownership Dispute attack
(B) Watermark removal attack
(C) Invertible watermark attack

4.1 Ownership Dispute Attack

In case buyer obtains a copy of I_{OI} and if the buyer tries to watermark it again by using his watermark to get the watermarked image I_{OBI}. Now the buyer can claims himself the legal owner. Ownership dispute between owner and buyer over I_{OBI} becomes an

attack now. Since the watermarking technique used in "Ownership Identity Watermarking Protocol" is robust the attack can easily be solved. It is clear that both owner's and buyer's watermarks can be detected in the disputed image I_{OBI} as we have used the DCT-SVD domain image watermarking technique. Buyer with his forged original I_{OBI} can show the presence of his watermark in I_{OBI}. However, he cannot prove the presence of watermark in owner's original image I. Where as owner can prove the presence of his watermark both in buyer's forged original and at the same time in the forged watermarked Image I_{OBI}. Thus the Robust watermarking chosen helps the owner to prove the legal ownership of I_{OBI}.

4.2watermark Removal Attack

When a situation arises that the Buyer performs some operation on owner's watermarked image I_{OI} to get another image $\hat{I}$ such that that the strength of W_{OI} in $\hat{I}$ is condensed such that W_{OI} can not be detected in $\hat{I}$. Then Buyer sends $H(I)$ to the CA along with a request for a digital signature. Suppose the CA sends Buyer the digital signature, it is sensible to assume that the time stamp of owner should be lesser than Time Stamp of Buyer, since Buyer can only obtain $\hat{I}$ after owner generates I_{OI}.

Owner and Buyer produce their original images I and $\hat{I}$ along with their respective watermark certificates. The judge will verify whether the identities of owner and Buyer are connected with their respective watermark certificates.

The time stamp of Buyer (TS_2) and actual owner (TS_1) are extracted from the certificates by the judge. The judge will then make a decision about the actual owner by comparing the time stamp. Since owner got before Buyer, $TS_1 < TS_2$. As a result, owner will be considered the true owner and Buyer will fail to prove his false claim of ownership.

4.3 Invertible Watermarking Attack

The first attack portrays a situation which owner will claim his legal ownership because Buyer cannot prove the presence of his watermark in owner's original image I. If Buyer is able to prove the presence of his fake watermark in owner's original image it becomes an issue. Craver et al. [9] have discussed these situations. If the buyer is smart enough to subtract a watermark W from I_{OI} to get image I_{OI} which he calls his original. owner's watermarked image and buyer's fake original are represented as

$$I_{OI} = I + E_{K_O^{pub}}(W_{OI}) \quad (21)$$

$$\hat{I}_{OI} = I_{OI} \triangleright W = (I + E_{K_O^{pub}}(W_{OI})) \triangleright W \quad (22)$$

From the above two equations

$$I_{OI} = (\hat{I}_{OI} \triangleleft W) \quad (23)$$

$$I = (\hat{I}_{OI} \triangleright W_{OI} \triangleleft W) \quad (24)$$

Where $\triangleleft$ denotes embedding and $\triangleright$ denotes extraction of watermark.

We find that by using his fake original $\hat{I}_{OI}$, Buyer can prove the presence of his watermark W both in owner's watermarked Image I_{OI} and owner's original image I. Buyer can therefore indict owner that I_{OI} and I are undeniably his copies of the watermarked image I_{OI}. The owner can show his watermark in I_{OI} and I_{OI}. Craver et al. [9] have termed such a scheme as *invertible*, To solve this problem, Craver et al.[9] suggested the Hash the original image to get a seed. The watermark is generated using this seed with a fixed pseudorandom number generator,

But, Ramkumar et al. [10] have shown that this method is still invertible. With our proposed protocol, however, an invertible watermark attack does not seem possible because the watermark requires the private key of the owner which is known only to the owner.

5. Conclusion

Since the watermarking techniques alone are not adequate in catering to the complex issues in copyright protection issues, integrating another stronger technique proves inevitable. Even the usage of public and private keys of owners and buyers as watermarks poses the threat of compromising the security. If the encryption technology implemented is unraveled, and the problems out of deciphering the public-private keys of the party involved would lead to cascading catastrophic repercussions. Hence the proposed watermarking method chose to watermark the hash value derived from the original document and encrypt using only the public key of the owner. It is pre-requisite to have the knowledge of the private key of the owner to decrypt the watermark. Even if the decrypted message is extracted, proving the hash value impose an

indomitable challenge, as the chances of deriving a similar hash value is practically immaterial, without the original document. Unwarrantedly the original document lies only with the genuine owner. Moreover the public key of the watermark is indisputably associated to the owner not just of its uniqueness, but also being registered from a registering authority.

Copyright Infringement issues are solved through the proposed concept by the way of imprinting the hash value derived from a combination of the public keys of the buyer and the owner. This process provisions the identification of authentic buyer and also helps to trace the buyer from whom the unauthentic duplicate copies emerged, in case of copyright infringement issues. The need for registration of public keys with a registering authority after receiving it from the certificate authority leaves no room for it being claimed by other people, legally. This concept by all means helps to solves issues pertaining to buyer-owner identification, copyright infringements and Ownership Dispute Attack.

References:

[1] Doerr, G. and Dugelay, J.-L. (2003) A Guide Tour of Video Watermarking. *Signal Processing: Image Communication, Special Issue on Technologies for Image Security*, 18 (4). pp. 263-282.

[2] M.Holiman and N.Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes," *IEEE Trans. Image Process*, vol.9, no.3, pp.432–441, 2000.

[3] Memon, N. and Wong, P. (1998). Protecting Digital Media Content. *In: Communications of ACM*, pp. 35-43, Vol. 41, No. 7, July 1998

[4] G. Voyatzis and I. Pitas, "The use of watermarks in the protection of digital multimedia products," *IEEE Proceedings*, vol. 87, No. 7, pp 1197-1207, July 1999.

[5] A.B. Kahng, J. Lach, W.H. M-Smith, S. Mantik, I.L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, "Constraint-based watermarking techniques for design IP protection," *IEEE Trans. Comput.-Aided Des. Integrated Circuits Syst.*, vol.20, no.10, pp.1236–1252, Oct. 2001.

[6] Fernando Perez-Gonzalez and Juan R. Hernandez, "A tutorial on digital watermarking," Security Technology, 1999 Proceedings. *IEEE 33rd Annual International Carnaban Conference on 1999*, pp. 286-292, 1999

[7] F. Mintzer and G. W. Braudaway, "If one watermark is good, are more better?" in *IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 4, pp. 2067–2069, Phoenix, Ariz, USA, March 1999.

[8] A. Sverdlov, S. Dexter, and A. M. Eskicioglu, "Robust DCT-SVD Domain Image Watermarking for Copyright Protection: Embedding Data in All Frequencies," submitted to *Multimedia Computing and Networking 2005 Conference*, San Jose, CA, January 16-20, 2005.

[9] S. Carver, N. Memon, B.-L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 573–586, 1998.

[10] M. Ramkumar and A. N. Akansu, "Image watermarks and counterfeit attacks: some problems and solutions," in *Proceedings of Content Security and Data Hiding in Digital Media*, Newark, NJ, USA, May 1999.

[11] J. Bloom et. al., "Copy protection for DVD video," *IEEE Proceedings*, vol. 87, No. 7, pp 1267-1276, July 1999.

[12] J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, 1997.

[13] T. Furon and P. Duhamel, "An asymmetric watermarking method," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 981–995, 2003.

[14] J. J. Eggers, J. K. Su, and B. Girod, "Public key watermarking by eigenvectors of linear transforms," in proceedings of the *European Signal Processing Conference (EUSIPCO '00)*, Tampere, Finland, September 2000.

[15] N.Memon and P.W.Wong, "A buyer-seller watermarking protocol," *IEEE Transactions on Image Processing*, vol. 10, no. 4, pp. 643–649, 2001.

[16] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[17] Neil F.Johnson, Zoran Duric and Sushil Jajodia, "Recovery of Watermarks from Distorted Images," Proceedings of the *Third Information Hiding Workshop*, - Dresden, Germany - October 1999.

[18] J. R. Smith and B. O. Comiskey. "Modulation and Information Hiding in Images". In Proceedings of *International Workshop on Information Hiding*, Cambridge, UK, May 1996 pp 39-48.

[19] J. Zhao and E. Koch, "Embedding Robust Labels into images for Copyright Protection," *Intellectual Property Rights and New Technologies, Proceedings of the KnowRight'95 Conference* 1995, pp. 242-51.

[20] M. L. Miller, "Is asymmetric watermarking necessary or sufficient?" in Proceedings of the *European Signal Processing Conference (EUSIPCO '02),* Toulouse, France, September 2002.

[21] M.Ramkumar and A. N. Akansu, "A robust protocol for proving ownership of multimedia content," *IEEE Transactions on Multimedia*, vol. 6, no. 3, pp. 469–478, 2004.

[22] S.Katzenbeisser, "On the integration of cryptography and watermarks," in *International Workshop on Digital Watermarking*, vol. 2939 of Springer Lecture Notes in Computer Science, pp. 50–60, Seoul, Korea, October 2003.