Watermarking On Compressed & Encrypted JPEG 2000 Images Using Rational Dither Modulation

K. P. Tayade, S. S. Bobde

Abstract*— Rational Dither Modulation (RDM) is an efficient method of watermarking which is sensitive to variations in the amplitude of signals. In the digital world, images are available in various formats. They are simple to copy and resell without any loss of quality. In Digital Asset Management System (DAMS), media data is handled in compressed and encrypted form. It becomes necessary to watermark this form of data to copyright management purpose, ownership declaration and tamper detection. By watermarking the compressed and encrypted data, there is degradation of an image quality. Rational Dither Modulation is an alternative to Quantization Index Modulation with volumetric invariance. In the proposed scheme, using compression, the information of raw media is packed and an encryption algorithm randomize the compressed bit stream. Rational Dither Modulation embeds watermark in the compressed and encrypted domain and extraction of watermark can be done in encrypted and decrypted domain. The digital media is often distributed by multiple levels of distributors in encrypted and compressed form. Rational Dither Modulation investigates security, perceptual quality, embedding capacity and robustness.

Index Terms*— Rational Dither Modulation, Spread Spectrum, Scalar Costa Scheme and Quantization Index Modulation, Digital Right Management, JPEG2000, Stream Cipher.

I. INTRODUCTION

Rational Dither Modulation is the watermarking method which is used to provide robustness against amplitude scaling attacks and minimizes Bit Error Rate. It is very difficult to perform watermarking on the compressed and encrypted data. The Rational Dither Modulation Algorithm is simple to implement as it is directly performed in the compressed encrypted domain. In the proposed system, the source image is first compressed using standard JPEG2000 compression which include discrete wavelet transform then the output after compression is encrypted using RC4 cipher. RC4 cipher converts the image data into byte stream. The output from the process of encryption is then watermarked with Rational Dither Modulation scheme. After watermarking, the streamed data is then sent to receiver side through network. At the receiver side, the streamed data is first decrypted using key of RC4 cipher. Then it is uncompressed with JPEG2000 decoder. After that watermark signal is detected. The proposed algorithm uses a symmetric stream cipher with additive homomorphic properties for encryption.

Manuscript received September, 2013.

Mr. Krishna P. Tayade, Student, Department of Computer Engineering, Maharashtra Institute of Technology, Kothrud, Pune, University of Pune, India.

Prof. S. S. Bobde, Department of Computer Engineering, Maharashtra Institute of Technology, Kothrud, Pune, University of Pune, India.

Digital asset management systems (DAMS) normally operate on media data in a compressed and encrypted form. It becomes essential to watermark these compressed encrypted data items in the compressed-encrypted domain itself for tamper detection or ownership declaration or copyright management purposes.[1] It is a challenge to watermark these compressed encrypted streams as the compression process would have packed the information of raw media into a low number of bits and encryption would have randomized the compressed bit stream.In DRM systems with content owners, multiple levels of distributors and consumers, the distributors do not have access to plain content (un-encrypted content). As they are distributors of content who distributes the encrypted content (in fact compressed encrypted content as most of the content would be compressed and then encrypted) and requests the license server in the DRM system to distribute the associated license containing the decryption keys to open the encrypted content to the consumers. [4] In fact distributors do not need to have plain content as they are not consumers. However the content for media is used for proving the distributorship by the distributor. Thus they have no choice but to watermark in the compressed encrypted domain.

Intellectual property issues are raised by the widespread use of the Internet. After content is downloaded, no further protection is provided on that content. DRM (Digital Rights Management) technologies were developed to ensure the protection of digital information.[4] Digital rights management (DRM) systems involve two party systems which contain the owner and consumers. For scalability of business, it is important to add levels of distributors and sub-distributors who can distribute and promote the content in regions unknown to the original owner. Thus, the architecture is proposed for multiparty multilevel DRM system.

A. Motivation

In existing system, sometimes sender add watermark by using the reformation of bits. So, the image quality is decreased as well as if some change in the bits at the time of compression, there is large variance in the image quality. The same is for encryption process. To overcome this problem, in the proposed system the image is first compressed and then encrypted and lastly it is watermarked to maintain a quality of image.

B. Need

In this scheme, a robust watermarking technique is proposed for JPEG2000 images, in which the watermark can be embedded in a predictable manner by exploiting the homomorphic property of the cipher. Watermarking in compressed encrypted content saves the computational complexity and preserves confidentiality of the content.

C. Background

There have been several related image watermarking

techniques proposed to date. Deng et al. proposed an efficient buyer-seller watermarking protocol based on composite signal representation. However, when the content is accessible only in encrypted form to the watermark embedder, the embedding scheme proposed might not be applicable as the host and watermark signal are represented in composite signal form using the plain text features of the host signal, this is possible as the seller embeds the watermark. Also, there is a cipher text expansion of 3.7 times that of plaintext. Some sub-bands of lower resolutions are chosen for encryption while watermarking the rest of higher resolution sub-bands. While in other scheme, the encryption is performed on most significant bit planes while watermarking the rest of lower significant bit planes. In case lesser number of sub-bands/bit planes are used for encryption, an attacker can manipulate the un-encrypted sub-bands/bit planes and further extract some useful information from the image, although the image may not be of good quality. On the other hand, if more sub-bands/bit planes are encrypted and only rest few sub-bands/bit planes are watermarked, it might be possible for an attacker to remove the watermarked sub-bands/bit planes while maintaining the image quality. [3]

II. LITERATURE SURVEY

A. DAMS

Digital asset Management System uses protocol for grouping, archiving, optimizing, downloading, maintaining, reforming and sending files in encrypted and compressed type. [2] It consists of management tasks and choices encompassing the uptake, annotation, storage, retrieval and distribution of digital assets. Digital pictures, animations, videos and music exemplify the target areas of media plus management.

The following broad classes of digital asset management systems could also be distinguished as:

1. Brand asset management systems concentrate on facilitation of content re-use among massive organizations. Here the content is essentially marketing or sales related, for instance, product representational process, logos, promoting collateral or fonts, to present many examples.
2. Library asset management systems concentrate on storage and retrieval of huge amounts of occasionally dynamic media assets, for instance in video or icon archiving.
3. Production asset management systems concentrate on managing assets as they're being created for a digital media production (video game, 3D picture show, animation, visual-effects shots, etc.). They sometimes embrace work-flow and project-management options as well as the storage, organization and revision management of often dynamic digital assets.

B. DRM

It is the system of distribution of media content during a compressed & encrypted format to consumers through hierarchical distributor network. Multiparty structure digital rights management (DRM) design involving many levels of distributors in between associate owner and a consumer has been advised as an alternate business model to the standard two-party (buyer-seller) DRM design for digital content delivery. In the two-party DRM design, techniques are used for secure delivery of the content. The protocols employed in the two-party case for secure content delivery may be directly applied to the multiparty structure case. However, the watermarking protocols employed in the two-party case might not directly carry over to the multiparty structure case, because it has to address the synchronous security issues of multiple parties like the owner, multiple levels of distributors and end user. This scheme takes care of the safety issues of all parties concerned. The protocol is also improved to scale back the dependence on the license server.

C. Buyer Seller Watermarking Protocol

It is based on composite signal illustration where content is accessible solely in encrypted type to the watermark embedder & the watermark signal are depicted using features of plain text. Digital watermarks have recently been projected for the needs of copy protection and replica deterrence for multimedia content.[9] In copy deterrence, a content owner (seller) inserts a novel watermark into a duplicate of the content before it's sold to a client. If the customer sells unauthorized copies of the watermarked content, then these copies is derived to the unlawful reseller (original buyer) employing a watermark detection formula. One drawback with such scheme approach is that the initial client whose watermark has been found on unauthorized copies will claim that the unauthorized copy was created or caused (for example, by a security breach) by the initial vender. The scheme propose an interactive buyer–seller protocol for invisible watermarking during which the vendor doesn't get to understand the precise watermarked copy that the customer receives. Therefore the vendor cannot produce copies of the initial content containing the buyer's watermark. In cases where the vendor finds an unauthorized copy, the vendor will determine the customer from a watermark in the unauthorized copy, and moreover the vendor will prove this reality to a third party employing a dispute resolution protocol. This prevents the customer from claiming that an unauthorized copy might have originated from the vendor. The watermark embedding protocol is predicated on public key cryptography and has very little overhead in terms of the overall knowledge communicated between the customer and therefore the vender.

D. Quantization Index Modulation

In this technique, the addition or subtraction of a watermark bit to a sample is predicated on the worth of measure plaintext sample. The watermark embedder doesn't have access to the plain text values. They need solely compressed-encrypted content & don't have the key to un-encrypt and obtain the plain text compressed values. Copyright notification, authentication and applications like digital audio broadcasting are examples of emerging multimedia system applications for digital watermarking. It derive information-embedding capacities for the case of coloured Gaussian host signal and additive colored Gaussian noise attacks. These results imply an info embedding capability of about 1/3 b/s of embedded digital rate for each Hertz of host signal information measure and each decibel drop in received host signal quality. QIM is important optimum embedding strategy against some necessary classes of intentional attacks similarly.

E. Content Dependent Watermarking

It embeds the watermark in an encrypted format, however the host signal continues to be in the plain text format but the

distortion introduced in the host signal may be giant. A distortion sensitivity of the image content is decided by analyzing the cover object in both spacial and frequency domains. Local information that is derived from properties like texture, corner, edge is employed to work out a mask of simply noticeable difference values. The value which depend on the image content, gives the strength of the watermark information which will be embedded. It uses a much better technique of detecting edges using part congruency, allowing to detect a lot of edges accurately. The scheme implements an algorithm that detects corners using curvature scale space. The detected corner is employed as an element to determine the uniform regions in the image that is used to see the differential threshold mask. The robustness of scheme to JPEG compression is found to be smart at a high quality. The results for alternative image process attacks like median filtering and contrast sharpening filter were additionally found to be sensible, though it's not terribly robust against scaling and high noise levels.

F. Semi Fragile Authentication System

This scheme is not fully compressed and encrypted domain watermarking compatible as it derives the content based features for watermarking from the plain text. Semi-fragile image authentication deals with verifying authenticity of a received image while allowing some acceptable manipulations. In a semi-fragile authentication watermarking solution was proposed for JPEG images. JPEG-specific invariant features are identified and used for image signature generation and embedding. Semi-fragile authentication of JPEG2000 images under a generic framework which should pass authentication are defined based on considerations of some target applications. It operates on lowest authenticable bit rate – images undergoing repetitive re-encoding are guarantee to pass authentication provided the re-encoding rates are above the lowest allowable bit rate.

G. Spread Spectrum

The watermark signal for SS is generated without using host data. In the context, security is known because the issue of estimating the secret parameters of the embedding function supports the observation of watermarked signals. On the theoretical aspect, the security is quantified from an information-theoretic purpose of point by means of the equivocation about the key parameters. The main results reveal basic limits and bounds on security and provide insight into different properties like the impact of the embedding parameters, and the tradeoff between strength and security. On the practical side, executable estimators of the key parameters are projected and on paper analyzed for a range of situations, providing a comparison with previous approaches, and showing that the protection of the many schemes employed in practice are often fairly low. The protection of spread-spectrum-based data-hiding strategies has been investigated from theoretical and practical points of view.

H. SCS

Research on data hiding techniques has received substantial attention because of its potential application in multimedia system security. Digital watermarking is an information hiding technique wherever the embedded information is powerful against malicious or accidental attacks, may provide new potentialities to enforce the copyrights of multimedia system data. The initial knowledge isn't available to the decoder. For Gaussian data, in 1983, Costa projected a scheme that in theory achieves the capability of this communication situation.[7] but, Costa's scheme isn't practical. Thus, many analysis teams have projected suboptimal practical communication schemes based on Costa's plan.

The goal of scheme is to present an entire performance analysis of the scalar Costa scheme (SCS), that may be a suboptimal technique using scalar embedding. Information theoretic bounds and simulation results with progressive committal to writing techniques are measured. Further, amplitude scaling attacks and the invertibility of SCS embedding square measure investigated. Information embedding into IID original data and an attack by AWGN has been investigated. The decoder has no access to the original data. This situation may be considered to be communication with side information at the encoder that a theoretical communication scheme has been derived by Costa in 1983.

I. SCS-QIM

The watermark signal can be detected before and after decryption in the compressed domain which is a suboptimal technique using scalar embedding and reception functions. Eggers et al. proposed SCS scheme for watermark embedding. In this scheme, given a watermark strength, quantizer is used to ensemble of quantizers to embed the watermark.

J. Rational Dither Modulation

It is a quantization-based data-hiding technique that is basically liable to amplitude scalings and modifies it in such a way that the result becomes invariant to realize attacks. [6] This technique retains most of the simplicity of the traditional dither modulation (DM) scheme. RDM is predicated on employing a gain-invariant adaptive approximation step-size at each encoder and decoder. This causes the watermarked signal to be asymptotically stationary. Mathematical tools are used to verify the stationary probability density function that is later used to assess the performance of RDM in Gaussian channels. RDM is compared with improved spread-spectrum methods, showing that the previous can do a lot of higher rates for an equivalent bit error probability. RDM could be a novel data-hiding technique that's invariant to fixed gain attacks and doesn't need estimating the step-size, as most existing methods do. RDM constructs a gain-invariant domain in which quantization takes place, and it will so in a very simple manner, amounting to minor modifications of the quality DM technique.

III. PROPOSED WORK

A. Problem definition

To implement watermarking using Rational Dither Modulation (RDM) on compressed and encrypted data.

B. Scope

To maintain the quality of the image of compressed and encrypted format when it is received at receiver side by minimizing bit error rate and noise.

C. Goal

Goal of the proposed system is to secure the distribution of digital data by using rational Dither modulation along with

embedding capacity, robustness and perceptual quality.

D. Objective

1. To give a watermarking scheme which is robust against noise attack and scaling attack.
2. To secure data in compressed format.
3. To minimize Bit Error Rate of watermarked signal.
4. To provide necessary mechanism for traitor tracing, copyright management and distributor protection against false implication.

Project Goal	Priority	Description
Functional Goals:		
Confirmation of sender	1	Sender confirmation using Watermarking.
Maintaining Confidentiality	2	Check if third party is decrypting the data.
Technological Goals:		
Use of effective Watermarking Technique	1	Reduce the Bit Error Rate, Noise and Scaling attack.
Quality Goals:		
Non-repudiation	1	No one other than sender can claim about the sent data.
Security	2	The data should be secured.
Constraints:		
Encryption Algorithm	1	RC4 is having some limitations

E. Constraint

RC4 has weaknesses that argue against its use in new systems. It is especially vulnerable when the beginning of the output keystream is not discarded or when nonrandom or related keys are used; some ways of using RC4 can lead to very insecure cryptosystems such as WEP (Wired Equivalent Privacy). If some other cipher is used which is having advantages over RC4 then the scheme will work on wireless distribution media very effectively.

IV. RESEARCH METHODOLOGY

The proposed algorithm works on JPEG2000 compressed code stream. JPEG2000 compression is split into five totally different stages. In the initial stage the input image is preprocessed by dividing it into non-overlapping rectangle sized tiles, the unsigned samples are then minimized by a constant to create it bilaterally symmetrical around zero and eventually a multi-component transform is performed. Within the second stage, the distinct wavelet transform (DWT) is applied followed by quantization within the third stage. Multiple levels of DWT provide a multi-resolution image. The lower resolution contains the low-pass image whereas the highest resolutions contain the high-pass image. These resolutions are more divided into smaller blocks called code-blocks wherever every code-block is encoded separately. After that the quantized DWT coefficients are divided into completely different bit planes and coded through multiple passes at embedded block coding with optimized truncation (EBCOT) to present compressed byte stream within the fourth stage.[8][1] The compressed byte stream is organized into completely different wavelet packets based on resolution, precincts, elements and layers in the fifth and end. Thus, it's possible to pick out bytes generated from different bit planes of various resolutions for encoding and watermarking.

The proposed algorithm uses a symmetric stream cipher with additive homomorphic properties for encryption. In fact the distributors get JPEG2000 compressed stream cipher encrypted images for distribution. The distributors can then embed Rational Dither Modulation watermarking technique to this compressed encrypted stream. Rational Dither Modulation (RDM) is used for the purpose and study the bit error rate of detection and the quality versus payload capacity trade-off. Figure. 3.1 shows the watermark embedding and Fig. 3.2 gives watermark detection pipelines. The watermark signal for RDM is generated using C as shown with dashed-dotted line in the embedding block. The watermark signal detection can be done at any stage before and after the decryption module but in the compressed domain.

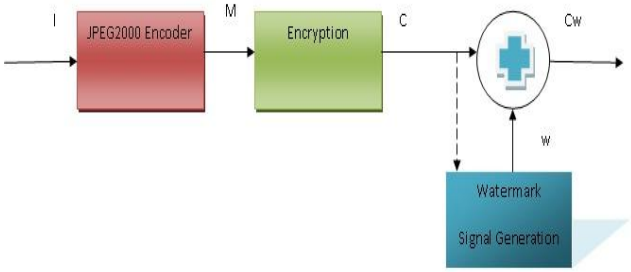

Figure 4.1: Watermark embedding

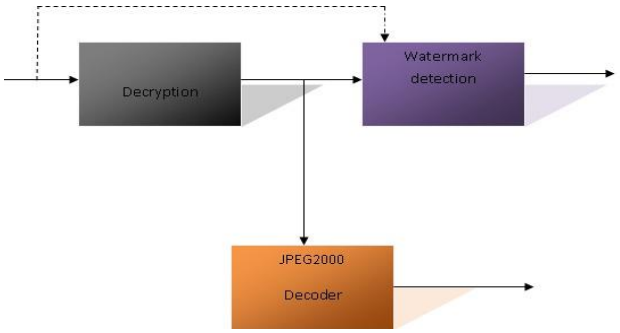

Figure 3.2: Watermark extraction.

A. Encryption Algorithm

JPEG2000 gives out packetized byte stream M as its output. In order to encrypt the message M, K is chosen, a randomly generated key-stream using RC. Then the encryption is done byte by byte to get the ciphered signal C:

$$C = E(M, K) = C_i$$

$$C = (m_i + k_i) \bmod 255$$

where the addition operation is arithmetic addition. Here, mod 255 is required to preserve the format compliancy of JPEG2000 bit stream. In JPEG2000 bit stream, the header syntax occurs as a value greater than 0xff89. This value corresponds to two consecutive bytes having values 255 and higher than 137 in decimal base. If mod 256 is used, it may generate a value 255 and the consecutive byte value greater than 137, which corresponds to syntax and is undesirable. So

to prevent the generation of header segments, the value mod 255 is used.

Let

$C_1 = E(M_1, K_1)$ and

$C_2 = E(M_2, K_2)$.

For $K = K_1 + K_2$,

additive homomorphism property gives

$$D(C_1+C_2, K) = M_1+M_2$$

Here, M_1 has been preprocessed by the owner. The owner does the preprocessing by limiting the values as $M_1 \mid M_1 \varepsilon [\alpha, 255 - (\alpha + 1)]$, where α is a positive integer. However, the preprocessing is not applied when $M_1 = 255$ and $M_{1i+1} > 137$, because this case indicates the presence of a header segment which should be preserved to preserve the bitstream compliance. Thus the stream cipher has additive privacy homomorphism property. The privacy homomorphism property will make it possible to detect the watermark from the decrypted content and also help us to control the watermarked image quality easily.

The security of the cryptosystem lies on the underlying stream cipher used. RC4 is a stream cipher and its security has been investigated in depth. The compressed encrypted byte stream C is given to distributors to distribute. They do not have access to the original image. Often distributors need to watermark C to prove their distributorship to the recipient or copyright violation detection purposes.

B. Embedding Algorithm

The encryption algorithm used is an additive privacy homomorphic one, so the watermark embedding is performed by using a robust additive watermarking technique. Since the embedding is done in the compressed ciphered byte stream, the embedding position plays a crucial role in deciding the watermarked image quality. Hence, for watermarking, the ciphered bytes are considered from less significant bit planes of the resolutions, as inserting watermark in ciphered bytes from most significant bit planes degrades the image quality to a greater extent. As well as the higher resolutions are vulnerable to transcoding operations and lower resolution contains a lot of information, whose modification leads to loss of quality. The watermark can be inserted in less significant bit planes of middle resolutions without affecting the image quality much. Since the embedding and detection are done on integer domain, the watermark is added after rounding off to the nearest integer for RDM. The rounding off process decreases the watermark power or in other words introduces noise and its effect on detection performance.

Rational Dither Modulation

Gonzalez et al. proposed a watermarking scheme based on quantization of the ratio of host signal to a function g (.). The quantizers are given by

$$Q'\Delta = 2\Delta + w\Delta/2$$

where $w \varepsilon \{-1, 1\}$ is the watermark information to be embedded in the source element. The embedding rule can be defined as

$$C_{wi} = g(C_{wi-1})\, Q'\Delta\ (C_i / g(C_{wi-1}))$$

where C_{wi-1} and C_{wi} are the previous and current watermarked samples. Notice that C_{wi} is an amplitude enhanced version of scaled-quantized C_i. Thus following equation is possible,

$$W_i = C_{wi} - C_i$$

which gives the additive nature of watermark. The function g (.) is chosen such that the scheme is robust against amplitude scaling attacks and is given by

$$g(C_{wi-1}) = \left(\frac{1}{L_m}\sum_{j=i-L_m}^{i-1}\left|C_{w_j}\right|^{\gamma}\right)^{\frac{1}{\gamma}}$$

One of the drawbacks with this scheme is that the watermarked sample may differ from the original sample to a large extent due to the function g (.) used for quantization. So, g (.) is scaled by a constant factor known at both encoder and decoder to control the amount of watermark added. Thus, watermark embedding is carried out in compressed-encrypted domain, and the watermarked content is then distributed by the distributors.

C. Watermark Detection

The watermark can be detected either in encrypted or decrypted compressed domain or in uncompressed domain detection.

a. Encrypted Domain Detection

In encrypted domain, $\boldsymbol{C_W}$ is directly given to the watermark extraction module and the detection process is as follows. The detection of watermark is performed by the minimum distance criteria using the below equation,

$$w = \arg\min_{i-1}\left(\frac{C_{w_i}}{g(C_{w_{i-1}})} - Q^i\left(\frac{C_{w_i}}{g(C_{w_{i-1}})}\right)\right)^2$$

$\forall i = 1, \ldots L\text{-}1$

Here, gives two quantizers belonging to bits 1 and -1. The distance is computed corresponding to both the quantizers and the one which gives minimum distance gives the watermark bit.

b. Decrypted Domain Detection

The received compressed encrypted watermarked image is first passed through the decryption module to decrypt which defines the corresponding byte by byte decryption for the encryption. The received signal $\boldsymbol{C_W}$ is decrypted to give $\boldsymbol{M_W}$ as

$$\begin{aligned}\boldsymbol{M_W} = \boldsymbol{D}(\boldsymbol{C_W}, \boldsymbol{K}) &= (c_{w_i} - k_i) \bmod 255 \\ &\qquad \forall i = 0, 1, \ldots, L-1 \\ &= (c_i + w_i - k_i) \bmod 255 \\ &= m_i + w_i\end{aligned}$$

It can be seen from $\boldsymbol{M_W} = \boldsymbol{m_i} + \boldsymbol{w_i}$, the watermarked compressed byte stream is $\boldsymbol{M_W}$ merely addition of compressed byte stream $\boldsymbol{m_i}$, and the watermark signal $\boldsymbol{w_i}$. Thus by controlling the strength of $\boldsymbol{w_i}$, choice of resolution levels and bit planes, the quality of the watermarked signal could be easily controlled. The watermarked quality would be poor if more number of resolution levels is picked up and bit planes to watermark but the watermark embedding capacity would be high and vice versa.

c. Uncompressed Domain Detection

Let $\boldsymbol{I_{DW}}$, $\boldsymbol{I_{DU}}$, $\boldsymbol{I_{DWA}}$ denote decompressed-watermarked image, decompressed- original image & decompressed-watermarked-attacked image. Then the watermark signal in decompressed domain can be computed as $\hat{\boldsymbol{w}} = \boldsymbol{I_{DU}} - \boldsymbol{I_{DW}}$ and in case of attack, $\hat{\boldsymbol{w}} = \boldsymbol{I_{DU}} - \boldsymbol{I_{DWA}}$. For detection, a correlation measure between embedded and attacked watermark signal is computed as

$$\mathrm{corr}(\hat{W}_i, \check{W}) = \frac{E\left[\left(\hat{W}_i - \mu_{\hat{W}_i}\right)(\check{W} - \mu_{\check{W}})\right]}{\sigma_{\hat{W}_i}\sigma_{\check{W}}}$$
$$\forall i = 1, 2, \ldots, N_w$$

The correlation value against different watermarks is measured, i.e. it denotes the number of watermarks and the watermark with maximum correlation value gives the embedded watermark.

V. PROJECT DESIGN

A. Purpose

The purpose of the Software Requirements Specification (SRS) is to present the client a transparent and precise description of the practicality of the assessment-support software to be developed and to eliminate ambiguities and misunderstandings that may exist. For the client, the SRS can make a case for all functions that the software ought to perform. For the developer, it'll be a point of reference throughout software implementation and maintenance. The SRS divides the system needs into two components, behavioural and non-behavioral requirements. The behavioural requirements describe the interaction between the system and its environment. Non-behavioral requirements explain the definition of the attributes of the product which contain the extent of security, efficiency, dependability, maintainability, movability, capacity and therefore the standards of compliance of the product.

B. Scope

The scope of the project is to identify the best technique among the various for secure distribution of digital data. The algorithm is simple to implement as it does not require decrypting or partial decompression of the content. It also preserves the confidentiality of content as the embedding is done on encrypted data.

C. Overview

The SRS is organized into two main sections, the primary is the Overall Description and the second is that the Specific Requirements. Overall Description section of this document provides an outline of the functionality. It explains the informal requirements and is employed to provide a context for the technical requirements specification. Requirement Specification section of this document is primarily for the developers and gives technical terms and functionality of the product. Both sections of the documents describe an equivalent software product in its completeness.

D. Overall Description

Main focus is on watermarking of compressed-encrypted JPEG2000 images where the encryption refers to the ciphering of complete. Deng et al. proposed an efficient buyer-seller watermarking protocol based on composite signal representation. To watermark, content is accessible only in encrypted form. The embedding scheme proposed might not be applicable as the host and watermark signal are represented in composite signal form using the plain text features of the host signal, this is possible as the seller embeds the watermark. Rational Dither Modulation technique is used which embeds the watermark in the encrypted & compressed domain.

E. Software System Attributes

a. Key stream Generation

The keystream is generated at the encryption and decryption site using RC4 cipher. For encryption, a secret seed 'S' is applied to RC4 cipher to generate the keystream 'K'. In order to generates the same key 'K' at the decryption site, the seed 'S' must be delivered to the decryption site through secret channel.

b. Domain of encryption

The content is often distributed in this domain. The quality of the image drops drastically with increase in compression rate. However the encryption method does not affect the quality of the image and can be used for confidentiality.

c. Security of encryption algorithm

RC4 key stream behave like a truly random sequence which provides security. The size of a compressed data is not sufficient to clearly distinguish between RC4 cipher and truly random stream.

d. Security of Watermarking Algorithm

RDM is not robust against filtering attack. Collusion attacks can be made ineffective by using collusion resistant codes to identify groups of users involved in collusion.

e. Effect of scaling in RDM detection

The amount of watermark power embedded varies to great extent due to varying quantization step size. When the scale is decreased the watermark power increases which in turn decreases BER.

VI. CONCLUSION

1. The Algorithm is simple to implement as it is directly performed in the compressed encrypted domain.
2. It preserves the confidentiality of the content as the embedding is done on encrypted data.
3. The scheme controls the image quality while applying different operations on the image.
4. To get the better quality image after watermarking, bit planes with ($l < 7$) is used.
5. RDM provides robustness against amplitude scaling attacks & minimizes Bit Error Rate.

VII. FUTURE WORK

1. RC4 has weaknesses that argue against its use in new systems. It is especially vulnerable when nonrandom or related keys are used.
2. Some ways of using RC4 can lead to very insecure cryptosystems such as WEP (Wired Equivalent Privacy). If some other cipher is used which is having advantages over RC4 then the scheme will work on wireless distribution media very effectively.
3. The proposed scheme can be used for different compression techniques which is having higher performance than JPEG2000.
4. To improve the fidelity further by determining whether the neighboring block is sufficiently correlated to rely on its perceptual estimate and to examine techniques to more realistically handle clipping issues.

REFERENCES

[1] A. V. Subramanyam, Sabu Emmanual and Mohan S. Kankanhalli, "Robust Watermarking Of Compressed & Encrypted JPEG2000 Images", *IEEE Trans. On Multimedia*, vol. 14, no. 3,Jun. 2012.

[2] A. Subramanyam, S. Emmanuel, and M. Kankanhalli, "Compressed encrypted domain JPEG2000 image watermarking", *in Proc. IEEE Int. Conf. Multimedia and Expo, 2010*, pp. 1315–1320.

[3] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals", *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 180–187, Mar. 2010.

[4] T. Thomas, S. Emmanuel, A. Subramanyam, and M. Kankanhalli, "Joint watermarking scheme for multiparty multilevel DRM architecture", *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 758–767, Dec. 2009.

[5] Arvind Kumar Parthsarathy and Subhash Kak, "An Improved Method of Content Based Image Watermarking", *IEEE Trans. On Broadcasting*, Vol 53, No.2, Jun 2007.

[6] F. Perez-Gonzalez, C. Mosquera, M. Barni, and A. Abrardo, "Rational dither modulation: A high-rate data-hiding method invariant to gain attacks", *IEEE Trans. Signal Process.*, vol. 53, no. 10, pt. 2, pp.3960–3975, Oct. 2005.

[7] J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "Scalar costa scheme for information embedding", *IEEE Trans. Signal Process*., vol. 51, no. 4, pp. 1003–1019, Apr. 2003.

[8] YiweiWang, John F. Doherty, Robert E. Van Dyck "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images", *IEEE Trans. on Image processing* , Vol. 11, No. 2, Feb 2002.

[9] N. Memon and P. Wong, "A buyer-seller watermarking protocol", *IEEE Trans. Image Process*., vol. 10, no. 4, pp. 643–649, Apr. 2001.

[10] Khalid Sayood, "I*ntroduction to Data Compression"*, 3rd ed.

[11] Chih-Wei Tang and Hsueh-Ming Hang, "A Feature-Based Robust Digital Image Watermarking Scheme", *IEEE Transactions on Signal Processing*, vol. 51, no. 4, April 2003.

[12] Dalel Bouslimi, Gouenou Coatrieux, Michel Cozic, and Christian Roux, "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images", *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 5, September 2012.

[13] Xiangyang Wang, Jun Wu, and Panpan Niu, "A New Digital Image Watermarking Algorithm Resilient to Desynchronization Attacks", *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, December 2007.

[14] Qibin Sun and Shih-Fu Chang, "A Secure and Robust Digital Signature Scheme for JPEG2000 Image Authentication", *IEEE Transactions on Multimedia*, vol. 7, no. 3, June 2005.