Aim:

A study on combined cryptography and watermarking techniques.

Introduction:

Cryptography is a method of communication in such a way that only intended people can have access to the piece of information. Unauthorized people could not extract any information even if the cipher falls into their hands. The major importance of cryptography is to protect these three things about data: confidentiality which ensures that only authorized users have access to the transmitted data; integrity which verifies that the received data has not been manipulated by unauthorized users and authenticity, which proves that the received data comes from the correct source and the source does not deny it.

Watermark is a form of text or image that is impressed onto a text or image which provides evidence of its authenticity. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. A digital watermark is called robust with respect to transformations if the embedded information may be detected reliably from the marked signal, even if degraded by any number of transformations. Typical image degradations are JPEG compression, rotation, cropping, additive noise, and quantization. A digital watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, unwatermarked content. In general, it is easy to create either robust watermarks—or—imperceptible watermarks, but the creation of both robust—and—imperceptible watermarks has proven to be quite challenging.

A major limitation of pure cryptography is that the loss or deletion of the attached digital signature makes the data untrustworthy and thus it becomes hard to verify its integrity and authenticity. This suggests that cryptography can only be used as a priori protection mechanism. On the other hand, pure watermarking methods achieve security in telemedicine by using robust and fragile watermarks. Robust watermarks are characterized by their resistance to common signal processing and malicious attacks; thus, they are appropriate for ownership verification and identity authentication. On the other hand, fragile watermarks do not survive signal processing attacks, making them appropriate for data integrity control and tamper detection.

To utilize the combined benefits of the two approaches, crypto-watermarking algorithms have been proposed in literature to address the security requirement applications. In the hybrid approach, watermarking is used as the implementation platform, and integrity and authenticity are implemented using cryptographic watermarks such as hash codes, cyclic redundancy codes (CRCs), and digital signatures. These cryptographic watermarks are embedded as robust or fragile watermarks depending on the required security service. That is, hash codes are commonly used to provide strict integrity of the data, whereas CRCs are more appropriately used to detect tampered areas in the data.

Novel Applications:

Combined cryptography and watermarking algorithms are application dependent. Some of the techniques are suitable for specific applications, while the others are not well recognized yet but have a great potential. In the following table some applications are shown where combined cryptography and watermarking well fits to provide security protection.

Watermarking Techniques	**Related Novel Applications**
Robust	Copyright protection, Fingerprinting, Broadcast monitoring, Healthcare, Copy protection, e-Voting, Remote education
Fragile / Semi Fragile	Tamper proofing, Authentication and Integrity Verification, Covert communication
Blind	Copyright protection, Healthcare, Tamper proofing, Image authentication, Fingerprinting, Copy protection, e-Voting, Remote education
Semi Blind/ Non-Blind	Authentication and Integrity Verification, Covert communication

Issues in Combined Cryptography and Watermarking:

There are various issues in watermarking research. First issue is to maintain the balance between imperceptibility, robustness and capacity, as increasing one factor adversely affects the other and a good digital watermarking system possess the above feature. To achieve good imperceptibility, watermark should be embedded in high frequency component whereas robustness occurs in low frequency component. Currently, improving the robustness against attacks by protecting the visual quality is considered the core motivation of most existing watermarking schemes. Hence, the watermarking method can be successful if the low frequency mechanisms of the original message are used as the host for watermark insertion. Next one is payload size; it is the amount of information the watermark carries. As more payload size compromises with the imperceptibility. So, issue is how to maintain equilibrium. Next issue is robustness in spatial domain. As in spatial domain, there is change in pixel values. It hardly resists against various attacks like JPEG compression, high pass filtering, low pass filtering, cropping etc. Other issue is computational cost i.e., Cost of inserting and detecting watermark that should be minimized. Last one is we are using cryptography to enhance the security of data which may increase time density and complexity of system but it has negligible in compare to security level.

Summary Table:

Ref No	Proposed Objective	Used Technique	Considered Data		Results	Limitations
			Cover	Watermarking		
[1]	Robust crypto-watermarking technique for secure dissemination and protection of multispectral images	Arnold Transform / DWT / Multiplicative & transposition cipher	Different sizes of images (Color)	25x50 (Binary)	Max: PSNR=58.1853 dB, NC=0.9963 Against Attacks - Avg: NC=0.8945	> The proposed scheme is robust against most of the attacks except rotation attack (NC=0.6938).
[2]	Robust and imperceptible combined cryptography and watermarking scheme in frequency domain	DWT / SVD / Elliptic curve cryptography	512x512 (Grayscale)	32x32 (Binary)	Max: PSNR = 68.7505 dB at (Threshold value=0.002), NC=1 at (Threshold value=0.04) Against Attacks - Avg: NC=0.8986 at (threshold values=0.012), NC=0.9682 at (Threshold value=0.04)	> Threshold value have a specific breaking point, after that the nature of watermarked image is deformed and as its value increases, PSNR start to decrease but NC start to increase.
[3]	Robust and blind cryptography based watermarking algorithm in frequency domain for copyright protection of images	DWT / Visual Cryptography / scaled Odd/Even embedding technique	512x512x3 (Color)	64x64 (Binary)	Max: PSNR=44 dB & SSIM=0.997 at (Scaling factor=8), NC=0.99 at (Scaling factor=24)	> As the scaling factor strength increases, both PSNR and SSIM start to decrease but NC start to increase and rotation attack affects the small scaling factor much more than large scaling factor.
[4]	Robust, secure and hybrid cryptography and spatial domain watermarking technique for secure text message transmission	LSB / Fibonacci series / PN sequence / XOR cipher / RSA / Hill cipher	1024x768 (Color)	Text message of variable length	Max: PSNR=87.8982 dB Min: MSE=0.000106, RMSE=0.0103	> Time complexity of the system is increased due to an involvement of eight different types of encoders and decoders.

Ref No	Proposed Objective	Used Technique	Considered Data		Results	Limitations
			Cover	Watermarking		
[5]	Efficient joint encryption and reversible watermarking algorithm, for safe transmission of medical images	Histogram shifting/ AES/ Partial Encryption	2048x2048 (Grayscale)	300 × 300, 107 × 53 (binary)	Max: Payload Capacity= 2,013,444 PER=0.48 bpp Entropy= 7.99 PSNR=79.3223 dB	> Trade-off between maximum embedding capacity (highest in CT) and encrypted image entropy (highest in MRI/ X-RAY).
[6]	Imperceptible and blind cryptography based watermarking scheme in frequency domain, for copyright protection	Visual Cryptography/ DWT	256 x 256 (Grayscale)	128 x 128 (binary)	Max: PSNR = 38.57 dB NC = 0.9999	> The proposed work can be extended by using error correcting codes and filtering techniques.
[7]	More secure, robust and imperceptible watermarking mechanism in spatial domain based on cryptography	Symmetric key cryptography/ LSB/ bit pairs matching	512 x 512 (Grayscale)	32 x 32 (Grayscale)	Max: PSNR=52.992 dB, Payload Capacity= 534,266, UIQI=1 SSIM=1, MSSIM=1 Min: MSE=0.0031 Against Attacks - Avg: WPSNR=52 dB, NCC=1, SM=1, BER=0	> The proposed method is robust against most of the attacks except Gaussian attack (NCC=0.7, SM=0.75, BER=0.14) and Jpeg attack (NCC=0.7, SM=0.8, BER=0.09).
[8]	High capacity, joint encryption and reversible watermarking technique, for medical imaging security	Histogram shifting/ AES/ Partial Encryption/ Pixel Permutation	512×512 to 2048×2048 (Grayscale)	300 × 300, 305 × 98 (binary)	Max: Payload Capacity= 1,58,484 PER=0.605 bpp PSNR=58.8066 dB	> The achieved PSNR values decrease as the embedding payloads increase, and vice versa.

Ref. No.	Proposed Objective	Used Technique	Considered Data		Results	Limitations
			Cover	Watermarking		
[9]	Compression-Then-Encryption-Based Secure Watermarking Technique for Smart Healthcare System	CTE/RDWD-RSVD /SPIHT-SIE	512 x 512 Image	1). Encoded text watermark (168 bits) 2). Image Watermark (256 x 256)	1). Performance analysis of different images: Avg – 45.3362 dB (PSNR), 0.9893 (NC), 0.0 (BER) 2). Against Attacks: NC > 0.7, BER = 0 (except cropping attack, image scaling, and histogram Equalization)	>. Unacceptable ranges of NC and BER for attacks like cropping attack, image scaling, histogram equalization.
[10]	Keysplitting Watermark: Zero Watermark algorithm for Software Protection Against Cyber-Attacks This adds watermark to the code based on the inherent properties of the code	Blind code based zero watermarking	------	1). WM1 (370 characters) 2). WM2 (592 characters)	1). Watermark accuracy – 81% average 2). Watermark accuracy of attacked sample – 69.56% 3). Reduction in running time compared to two other models.	> Only applicable for text data i.e., code. > Currently for generic codes and not application specific.
[11]	Robust Watermarking Algorithm for medical volume data in Internet of Medical things.	3D hyperchaos /3D DTCWT – DCT/ Zero Embedding/ Blind Extraction	256 x 256	32 x 32 pixels	1). NC values for JPEG compression attacks till 15% - >0.80 2). During Gaussian attack, NC >0.95 when noise>=0.4 3). Under high intensity of attacks, NC curve very stable.	> In results of downward translation, NC values are not so good when dipped down to 15-20%.
[12]	A Novel Dual Image Watermarking technique using Homomorphic Transform and DWT	HT/DWT/SVD/AT	512 x 512	512 x 512	1). Max. PSNR and WPSNR – 60.2320 and 77.4798 dB 2). Max. SSIM – 0.9999 3). Max PSNR - 57.1796 dB after JPEG compression attack	> Not so effective against degree rotation attack

Summary:

In the paper [1], the authors proposed a crypto-watermarking technique for secure dissemination and protection of multispectral images. In the proposed algorithm, Arnold Transform is applied on watermark to increase security and robustness before watermark embedding. After this, watermark embedding algorithm uses scramble binary image as watermark and color multispectral image as a host image. Host multispectral image is decomposed up to third level for watermark embedding. Low-frequency and high-frequency sub-bands are selected for watermark embedding to achieve acceptable performance of imperceptibility and robustness. To provide security, Simple and strongly secure encryption based on multiplicative and two-stage transposition cipher is used. The proposed crypto-watermarking approach satisfies the security of encryption, the invisibility, robustness of watermarking. In the paper [2], an Elliptic Curve Cryptography centred encryption technique is used to encrypt the watermark and a DWT-SVD centred watermarking plan is used that explores 'U' part acquired in the wake of captivating the SVD of low frequency band under various threshold standards. In this technique, more prominent PSNR value at various thresholds illustrates that the nature of the watermarked image picture is better. And also give better results for jpeg images which are compressed and lossy in nature. In the paper [3], the authors proposed hybrid copyright protection technique. In this, firstly ownership watermark information is visually encrypted into 3 shares using visual cryptography algorithm, and then each shares of encrypted watermark information embedded into RGB layers of color cover images in the wavelet domain by using the discrete wavelet transform. First find 2 levels DWT decomposition of the RGB layers of cover image using 2D-DWT Haar wavelet then embed the visually encrypted shares of ownership watermark information in the lower frequency components block (LL2) using scaled Odd/Even embedding technique. In the paper [4], five different cryptography algorithms are used to encrypt five different segments of the text message and the encrypted text message is hide by LSB technique which enhance security of information by three levels, first one as finding the different algorithms which are implemented on different segments of the message which is extremely difficult by the intruder. Second, encryption of the data is using key, finding the one key of symmetric key cryptography and two keys: public key and private key of asymmetric key cryptography which is extremely difficult by the third party because these keys to maintaining the confidentiality of the message. Third, information is hiding by LSB watermarking, recovered the message by the third party is extremely difficult because LSB have enough capability against the intruder.

In the paper [7], the authors proposed a new cryptography-based bit pairs matching watermarking mechanism in the spatial domain and used the symmetric key cryptography to encrypt the watermark to protect the information from the intruder during transmission. The proposed mechanism improves the robustness of enhanced payload and security while maintaining the imperceptibility. In the papers [5,8], a technique based on reversible data hiding and cryptography is proposed. The proposed algorithm embeds two different watermarks simultaneously in two parts of the image; one in the spatial domain and another in the encrypted domain. Histogram shifting is used as an effective reversible data hiding scheme in both the papers to prevent any distortion in the medical image to ensure the right diagnosis. The overhead information is concatenated with the watermarked bits to make the algorithm blind. In paper [5] AES is used for cryptography and the image is divided into a large part and a small part, providing much higher payload in spatial domain than in encrypted domain. While in paper [8] AES/RC4 and pixel permutation are used for cryptography and the image is divided into two halves, providing higher payload in both the domains. The algorithm preforms well in terms of visual quality of the watermarked images and in terms of the available embedding capacity. This method also ensures the integrity, authenticity and confidentiality of the image before and after decryption, thus it can effectively be applied to medical images to provide security to the images during transmission or storage. In the paper [6], visual cryptography-based grayscale image watermarking in DWT domain is proposed for copyright protection. The watermark image is split into two shares using (2,2) VC scheme. One of the shares is registered with the trusted authority and other is embedded in the low frequency domain of host image after feature extraction. Finally, the extraction process recovers original watermark by performing XOR operation between the shares. The scheme satisfies the robustness, imperceptibility, blindness and security properties. This scheme can not only prove the ownership of image but also withstand various image processing attacks.

In the paper [9], a nonblind, dual watermarking technique is proposed that mainly comprises four major processes, i.e., watermark generation, insertion, CTE, and recovery of the generated watermark. This technique uses generated watermark where EPR data is first encoded using turbo code and then embedded into the wavelet coefficient of the watermark image. This generated EPR watermark is inserted into the redundant discrete wavelet transform (RDWT)-randomized Singular value decomposition (RSVD) coefficient of the cover image. In the paper [10], novel watermark-based algorithm is proposed for the protection of computer software against cyber-attacks. KeySplitWatermark first analyses software code to identify the keywords then make the partitions of the code on the basis of the selected keyword. The algorithm generates a unique key using the keywords and software code itself. If any copyright concern is raised in the future, this key can be used to demonstrate ownership. The embedding algorithm does not perform any tampering in software code to watermark it and extraction algorithms do not require watermark as input which makes it blind. The embedding algorithm generates the owner key as an output. That key is recorded with the CA and then further used to extract watermark. In the paper [11], a robust watermarking algorithm is proposed for medical volume data based on 3D DTCWT-DCT and hyperchaos scrambling. Since, when disease analysis and diagnosis images are three-dimensional, the data volume is large and analysis is relatively difficult. Along with that, due to the need of real-time diagnosis, its transmission speed cannot be sacrificed and the security of transmission must be guaranteed. To fulfil all the requirements, the algorithm is proposed according to perceptron model combined with the concept of hyperchaos scrambling algorithm, 3D DTCWT, perceptual hash and cryptography and applies the contour features of medical volume data to embed and extract watermark information. In the paper [12], the methodology proposed is a new technique of dual image watermarking is proposed for protection of ownership rights which utilizes salient properties of homomorphic transform (HT), discrete wavelet transform (DWT), singular value decomposition (SVD) and Arnold transform (AT). In embedding algorithm host image is split into reflectance and illumination components using HT, DWT is further applied to the reflectance component resulting in frequency sub-bands (HL and LH) which are transformed by SVD. Two image watermarks are selected for embedding process whereas security of proposed algorithm is strengthened by performing scrambling of second watermark through AT. Both watermarks are transformed with DWT and SVD. Singular values (SVs) of both transformed watermarks are embedded into SVs of host image.

References:

[1]. Secure Dissemination and Protection of Multispectral Images Using Crypto Watermarking https://ieeexplore.ieee.org/document/7274339

[2]. DWT-SVD based watermarking scheme of JPEG images using elliptic curve cryptography https://ieeexplore.ieee.org/document/7784981

[3]. Hybrid visual cryptography cum watermarking algorithm for copyright protection of images https://ieeexplore.ieee.org/document/7916858

[4]. A Hybrid Technique of Cryptography and Watermarking for Data Encryption and Decryption https://ieeexplore.ieee.org/document/7913175

[5]. Efficient Joint Encryption and Data Hiding Algorithm for Medical Images Security https://ieeexplore.ieee.org/document/7921962

[6]. Visual Cryptography based Grayscale Image Watermarking in DWT domain https://ieeexplore.ieee.org/document/8474621

[7]. On the implementation of a secured watermarking mechanism based on cryptography and bit pair matching
https://www.sciencedirect.com/science/article/pii/S1319157817305153

[8]. Medical Imaging Security Using Partial Encryption and Histogram Shifting Watermarking https://ieeexplore.ieee.org/document/8079950

[9]. Compression-Then-Encryption-Based Secure Watermarking Technique for Smart Healthcare System
https://ieeexplore.ieee.org/document/9093959

[10]. KeySplitWatermark: Zero Watermarking Algorithm for Software Protection Against Cyber-Attacks https://ieeexplore.ieee.org/document/9068217

[11]. Robust Watermarking Algorithm for Medical Volume Data in Internet of Medical Things https://ieeexplore.ieee.org/document/9094060

[12]. A Novel Dual Image Watermarking Technique Using Homomorphic Transform and DWT https://www.degruyter.com/document/doi/10.1515/jisys-2019-0046/html