I.J.Modern Education and Computer Science, **2012, 5, 10-17**
Published Online June 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2012.05.02

A Novel Technique for Copyright Protection of Images Using Hybrid Encryption Model

Swarnendu Mukherjee[1,a], Debashis Ganguly[2,b], Partha Mukherjee[3,c], Prasenjit Mitra[3,d]

[1]Cognizant Technology Solution, India
[2]Infosys Technology Limited, India
[3]Penn State University, USA

[a]mukherjee.swarnendu@gmail.com,
[b]DebashisGanguly@gmail.com,
[c]pmkrj2k@gmail.com,
[d]pmitra@ist.psu.edu

***Abstract*—**In this paper, we present a robust and novel strategic invisible watermarking scheme which can be used in the field of copyright protection. The novelty of our algorithm lies in the creation of a compound watermark image using the target image and the key image, where both of them are self encrypted. The self encryption concept adds an extra level of data security along with the security supported by the watermarking technique. Again, our method results a single invisible watermarked image which will be sent to the recipient and from that image, both the key and the target image can be extracted with no distortion using only the proposed extraction algorithm. Results of exhaustive experimentation using standard input color images demonstrate the robustness and efficiency of our approach.

***Index Terms*—**Authentication, content protection, cryptography, ownership identification. watermarking

I. Introduction

The rapid evolution of the Internet makes easier the transmission of digital multimedia content such as text, audio, images, and video. Digital media can be accessed or distributed through the network. As a result, copying is simple with no loss of fidelity, and thus the copy of a digital medium is identical to the original one. An unlimited number of identical copies of digital media can be illegally produced; this is a serious threat to the copyright of the media owner. Therefore, protection of intellectual property rights of the media owner is an important issue in the digital world.

Digital watermarking is a process of embedding data (watermark) into a multimedia object to help to protect the owner's right to that object. The embedded data (watermark) may be either visible or invisible.

In visible watermarking of images, a secondary image (the watermark) is embedded in a primary image such that watermark is intentionally perceptible to a human observer indicating the ownership of the image. Whereas in the case of invisible watermarking the embedded data is not perceptible, but may be extracted by a computer program [1].

In recent years, we have many watermarking tools to secure documents, information and also to maintain the originality and integrity of digital multimedia content. Most of existing invisible watermarking schemes are designed for either copyright protection or content authentication. Invisible watermarks can be broadly classified into two types, robust and fragile watermarks. Robust watermarks are generally used for copyright protection and ownership verification because they are robust to nearly all kinds of image processing operations. In comparison, fragile watermarks are mainly applied to content authentication and integrity attestation because they are completely fragile to any modifications. To fulfill multipurpose applications, several multipurpose watermarking algorithms based on wavelet transform and fast Fourier transform have been presented.

In this paper, we have presented a robust invisible watermarking technique to protect unauthorized access of data. When encryption techniques are used in conjunction with watermarking [2], protection from unauthorized access of digital content can be achieved. Our algorithm has been designed in such a way that it combines the concept of image encryption along with the watermarking scheme. Here, the message is watermarked immediately after creation. The sending party encrypts the watermarked content to provide the second layer of protection. At the receiving end, the stream is decrypted before watermark detection takes place. In our approach, use of cryptography protects the content while sending it through the network and the embedding of watermark implements ownership identification and the originality of the content.

II. Related Works

Huang et al. have developed [3] a watermarking scheme for the image ownership verification in terms of a private key pattern and wavelet filters. The watermarking is mainly achieved within the process of decomposition and reconstruction by forging watermark-carrying wavelet filters. But the proposed scheme is not robust against Noise addition, Cropping and distortion. If these factors are getting increased in the resultant image, then the proposed scheme fails to obtain the required pattern.

Anthony et al, [4] proposed an algorithm using the fast Hadamard transform (FHT) for the copyright protection of images. This algorithm can embed or hide an entire image or pattern as a watermark such as a company's logo or trademark directly into the original image. Authors have evaluated the performance of their algorithm using a benchmarking tool called Stirmark The experimental results shown in the paper claims that the suggested method can survive up to 60% of the Stirmark attacks. The proposed method has not been found to be so effective against random geometric transforms, such as shearing and general linear transforms. Also, it produces less acceptable results against the attacks like changing of Aspect Ratio, Compression and Scaling.

Hao et al, [5] presented a wavelet based watermarking technique that quantizes the so-called super trees for copyright protection. Embedding of each watermark bit is performed across diverse frequency bands. This feature enables the watermarking technique to resist the attacks in both frequency and time domains in a robust manner. Their results in their paper established the resistance of their system against attacks such as the removal of the highpass band in low-pass processing, and the removal of highpass details in JPEG compression. Moreover, they demonstrated the robustness to time domain attacks such as pixel shifting and rotation. In addition to protection of copyrights, their proposed watermarking scheme backs data hiding or image authentication.

R.J. Hwang [6] proposed a watermark method which is built up on the concept of visual cryptography in order to protect copyright ownership of digital image. According to the proposed method, the watermark pattern does not have to be embedded into the original image directly, which makes it harder to detect or recover from the marked image in an illegal way. It can be retrieved from the marked image without making comparison with the original image. The weakness of their proposed method is to use of different verification information for different watermarked images.

Cox et al. [7] has used spread spectrum techniques to embed watermarks in the DCT domain. To improve Cox's method, Lu et al. [8] did use cocktail watermarks which has improved the robustness and used HVS to maintain high fidelity of the watermarked image. The important issues such as the rightful ownership deadlock problem, the capacity problem, and the public-key detection problem will be considered in future research in addition to the robustness issue of watermarking addressed in their paper.

Lu et al. [9] presented a novel multipurpose blind digital image watermarking technique based on the multistage vector quantizer structure, which can be applied to both image authentication and copyright protection. They embed both semi-fragile and robust watermarks using different embedding techniques. The proposed method is fragile to most intentional attacks as their watermarking can endure few modifications.

Lu et al. [10] presented a multipurpose watermarking scheme which can be applied to attain both authentication and protection of multimedia data. The hiding process embeds the watermark once which can be extracted for diverse applications in the detection process, invisibly. The authors intend to verify data integrity as well to confirm the rightful ownership employing this multipurpose watermarking scheme. The efficiency of their watermarking scheme for content authentication and copyright protection is illustrated by the results. But, the use of multiple watermarks can result ownership deadlock as well as fingerprint problems.

Hu et al. [11] have proposed a reversible visible watermarking algorithm to satisfy a new application scenario where the visible watermark serves as a tag or ownership identifier, but can be completely removed to recover the original image data. It includes two procedures: data hiding and visible watermark embedding. In order to recover both the watermark-covered and non-watermark- covered image contents at the receiver end without any loss, the payload consists of two reconstruction data packets, one for recovering the watermark covered region, and the other for recovering the non-watermark-covered region. The data hiding technique reversibly hides the payload in the image region not covered by the visible watermark.

Tzeng et al. [12] presented an asymmetrical watermarking method for copyright protection that satisfies the zero knowledge principle with the intention to overcome the weaknesses of contemporary symmetric watermarking methods. The enhancement of the watermark space concept of their preceding symmetric watermarking method in their method made their asymmetric design a robust one. It is improbable to eradicate the watermark without visibly deforming the watermarked image owing to the significant dependence of their watermark on the original image.

In order to achieve the copyright protection, a two-phase watermarking scheme which extracts both the grayscale watermark and the binary one from the protected images was presented by Hu et al [13]. Initially, their scheme employed the pixel values of the original image to construct a grayscale watermark image. Then, their scheme intends to retrieve a binary watermark image by employing the just-procured-permuted grayscale watermark from the first phase. The outcome of their scheme is the lossless embedding i.e. the protected images and the original ones are identical when viewed. The authentication process in general does not necessitate the original image. Only the possessors of original grayscale watermark and the corresponding secret keys can extract the grayscale and binary watermarks in sequence. Thus, the system is enhanced in terms of security and robustness. Their proposed system fulfills the common necessities of image watermarking and is superior in comparison with the existing system in terms of transparency and robustness, which is demonstrated by the acquired results.

A novel watermarking scheme for copyright protection of color images was presented by Hsieh et al. [14]. The prerequisite of imperceptibility and robustness for a reasonable watermarking scheme has been fulfilled by their proposed scheme. The resistance of their scheme against numerous attacks for instance cropping, scaling, and JPEG compression, etc was illustrated by the experimental results. In addition, the ability of the scheme to extract unique features from diverse images, which is a vital prerequisite for feature extraction, was demonstrated by the unique identification experiment. The ability of their scheme to calculate the scaling factor for different images whilst preserving the robustness and imperceptibility requirement, which is in contrast to other watermarking schemes that require manual adjustment in the embedding scaling factor, is an additional advantage of their scheme.

Despite significant advances, research still needs to address many challenges related to attack resilience and robustness. Robustness of the watermarking techniques against several types of attacks is the main challenge in multimedia watermarking for copyright protection. And thus, invisible robust watermarking of digital images has become very crucial and important tool for network security, Content Protection and Copyright Protection. For easy identification of ownership, authentication, a source-based watermark like a unique identifiable color logo is more appealing.

Thus, we address the issue of strategically creating and implanting a watermark with the purpose of attack prevention, detection and ownership identification.

III. Our Works

To the best our knowledge, our work is the first attempt at introducing the concepts of encryption algorithms to hide the contents of an image file. Here we have coined a new term “PASSPIC”, which plays the same role that of the password or keyword in standard encrypting algorithms. This “PASSPIC” is used unaltered both in encryption and decryption. So, the whole algorithm is purely dependent on “PASSPIC”.

The algorithm of our proposed method is given below.

3.1. For Target File

3.1.1. For encryption.

1. Open the “PASSPIC” and the target file and read each pixel from them.
2. Split the pixels into RGB format and each RGB into 8 X 3= 24 bits.
3. Reverse each pixel of Target file. And make special XOR operation within the reversed byte and byte from “PASSPIC”.
4. Transpose the positions of the resultant bytes in cyclical manner.
5. Repeat the above steps.

3.1.2. For decryption.

1. Open the “PASSPIC” and the encoded target file and read each pixel from them.
2. Split the pixels into RGB format and each RGB into 8 X 3= 24 bits.
3. Transpose the positions of the bytes of encoded Target file in cyclical manner twice.
4. Make special XOR operation within the byte of transposed encoded target file and byte from “PASSPIC”. Reverse each pixel of Target file.
5. Repeat the above steps till you reach the end of the file.

3.2. For PASSPIC

3.2.1. For encryption.

1. Open the “PASSPIC” and read each pixel from it.
2. Split the pixel into RGB format and each RGB into 8 X 3 = 24 bits.
3. Follow GRR, GBB, RGG, and BGG for special XOR operation, i.e., first 2 bytes have gone through XOR and the result is stored in the second byte.
4. Follow step-2 and step-3 until the end of the file is reached.

3.2.2. For decryption.

1. Open the encoded “PASSPIC” and read each pixel from it.
2. Split the pixels into RGB format and each RGB into 8 X 3= 24 bits.
3. Substitute the positions between R and B.
4. Follow GRR, GBB, RGG, and BGG for special XOR operation, i.e., first 2 bytes have gone through XOR and the result is stored in the second byte.
5. Follow step-2 and step-3 and step-4 until the end of the file is reached.

3.3. For Watermark

3.3.1. For encryption.

1. Open the encoded “PASSPIC” and the Encoded target file and read each pixel from them.
2. Split the pixel into RGB format and each RGB into 8 X 3 = 24 bits.
3. Now check 8 bits at a time from encoded “PASSPIC”. If ‘1’ is present at a position then represent that position in Binary in Excess-3 Format else if there is ‘0’ then representing that position plain Binary 4-bit representation. Now put 8-bit from the encoded target file after them.
4. Continue step-2 and step-3 until the end of the file is reached.

3.3.2. For decryption.

1. Open the Watermarked Picture. Read each pixel from it.

2. Split the pixels into RGB format and each RGB into 8 X 3= 24 bits.
3. Now check 32 bits at a time and then check 4-bits in groups. If those 4-bits are in Excess-3 the convert it into plain Binary else keep it as it was. Then store it as encoded "PASSPIC".
4. Check next 8-bit of it and store it as encoded target file.
5. Continue step-3 and step-4 until the end of the file is reached.

Basically this encrypting and decrypting Algorithms for the target file consist of three basic standard functions –

1. Reversal implementing Transposition Technique.
2. Special XOR operation.
3. Cyclic replacement scheme using substitution technique.

After opening the "PASSPIC" and the target picture, we start reading the pixels of the two until the target file ends. Each pixel is split into its contents, i.e., R-G-B. The bits of each of the split bytes of the target files are, then, passed through (1), i.e., the reversal scheme and then (2) is followed, i.e., special XOR operation with the PASSPIC's bits then the R-G-B are shifted by (3) in circular fashion.

For decryption in the same way as above shown encryption it is required reopen the "PASSPIC" and the encoded BMP file. But now we have to first follow (3), i.e. , the cyclic displacement scheme twice and then we have to follow Special Exclusive-OR operation with the PASSPIC's bits and then transposition technique (1), and restore the pixels in a new picture that will be ultimately the same as our original file which was needed to be shared through network.

Now if we share the "PASSPIC" and the encrypted target file through network, it may occur that a crypt-analyzer getting the "PASSPIC" may crack the target file in its original format. But if we encode the "PASSPIC" too, then, it will be far more difficult to analyze the target file. So, to encode the "PASSPIC", we also require some algorithm. This algorithm also consists of Special XOR operation and Substitution technique. Similarly to decrypt it we follow the same way.

Now, to send these two encrypted image files we are taking help of Watermarking. Here, we are just enlarging the encoded "PASSPIC" using bitwise checking of positions of '1' and replacing it in EXCESS 3 FORMAT and embedding the encoded Target file in it.

From the algorithm it is pretty simple to get the idea that the encryption is depending on the nature of "PASSPIC" thrice for completion. So, for a hacker it is needed to search for the key or hit the algorithm thrice than the other existing ones.

IV. Results and Discussions

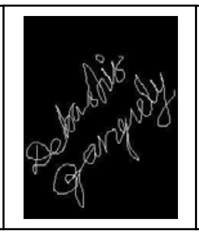
During our implementation phase, we have tested our algorithm for different sets of images. We considered different kind of images like: Chart, Map, Signatures, Logo and etc in our initial data set. The algorithm has shown good result for the entire data set. In this section, we are showing few good results.

A. *Performance analysis of the stated algorithm*

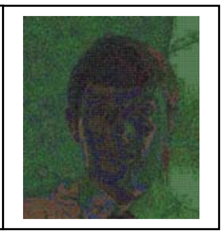
In our first experiment, we have considered a Digital Signature which can be watermarked with any kind of normal image. After applying our algorithm, the resultant Watermark image is also shown.

From the resultant image, it is clear that with out applying the proper decryption algorithm (as mentioned in our paper) along with the correct Passpic, it is impossible to obtain the original digital signature which has been embedded in it.

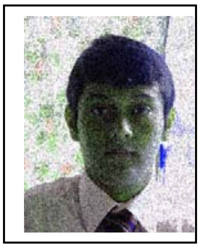
PASSPIC 1
FIGURE-1



TARGETPIC 1
FIGURE-2

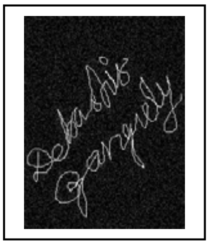


WATERMARK 1
FIGURE-3



PASSPIC 1
AFTER DE-WATERMARK

FIGURE-4

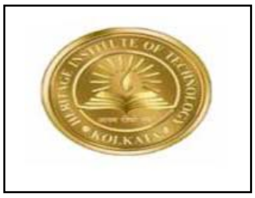


TARGET 1
AFTER EXTRACTION

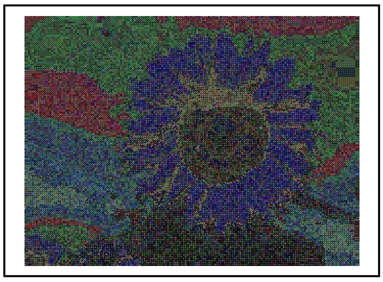
FIGURE-5

Our second experiment was performed on a Digital Logo image that can be watermarked behind any normal image before passing it through an untrusted network.

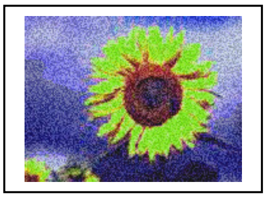
PASSPIC 2
FIGURE-6



TARGETPIC 2
FIGURE-7



WATERMARK 2
FIGURE-8



PASSPIC 2
AFTER DE-WATERMARK
FIGURE-9

TARGETPIC 2
AFTER EXTRACTION
FIGURE-10

To test the insertion of a watermark, we performed experiments on a large number of color images. The experiments revealed the efficacy of the proposed algorithm in producing watermarked images. It was observed that the typical execution time for insertion was 2.5sec on a Pentium 4 processor with a speed of 3:2GHz and 1GB memory for an image with a size of 256 X 256. Thus, the time overhead of the algorithm was minimal. The storage requirement overhead was also very small because of only the keys needed to be stored by the owner to prove ownership.

The memory requirement to store the keys is insignificant compared to the memory requirement of the host image.

The quality of the watermarked images using this method has been obtained using PSNR (Peak Signal to Noise Ratio) values in decibels (dB) given by the following expression [15]:

$$PSNR = 20\, log_{10}\left(\frac{255}{RMSE}\right) \quad \text{....... (1)}$$

where *RMSE* is the root mean square error of the watermarked image compared to the original image. The average PSNR value of the Figure-5 has been found to be 33dB and similarly the average PSNR value of Figure-10 has been found to be 29dB. From the above PSNR values it is clear that the output image produced in our method is having less distortion and thus it makes our method more stringent.

We have designed the scheme in such a way that it is inherently collusion attack resistant. As every watermark copy will have the different “policy”, attacker can not predict the watermark location and watermark data by colluding many copies of watermark image. Owner always has a record of different policies used to embed the watermark and can always extract the watermark data by supplying different policies while extracting a watermark from attacked watermark image. So after ensuring that our scheme is collusion attack resistant, we now need to check that our proposed scheme is robust against common image manipulations.

B. *Robustness Analysis*

We have conducted following image manipulations techniques over the watermarked images (Figure 3 and Figure 8) and then extracted the watermark:

Attack-1: Equalize the Histogram. This method usually increases the local contrast of many images, especially when the usable data of the image is represented by close contrast values. Through this adjustment, the intensities can be better distributed on the histogram.

Attack-2: Apply uniform scaling (Zoom). Scaling is a non-trivial process that involves a trade-off between efficiency, smoothness and sharpness. As the size of an image is increased, so the pixels which comprise the image become increasingly visible, making the image appears "soft". Conversely, reducing an image will tend to enhance its smoothness and apparent sharpness.

Attack-3: Adjust the brightness to +40 and contrast to +25. This method changes the image pixels to enhance its brightness and color contrast.

Attack-4: Adjust the hue and saturation to +10 each. The Hue/Saturation effect adjusts the hue, saturation, and lightness of individual color components in an image.

Attack-5: Add 10 % Gaussian noise. In Gaussian noise, each pixel in the image will be changed from its original value by a (usually) small amount. A histogram, a plot of the amount of distortion of a pixel value against the frequency with which it occurs, shows a normal distribution of noise.

Attack-6: Blur the image using Gaussian blur with 1 pixel radius. This method blurs an image using standard Gaussian function. It removes fine image detail and noise leaving only larger scale changes.

PSNR (dB)		
	Figure 5	Figure 10
Attack-1	36.03	27.01
Attack-2	31.20	28.60
Attack-3	30.10	26.80
Attack-4	35.63	27.62
Attack-5	32.14	28.75
Attack-6	35.02	30.03

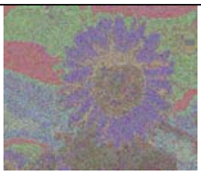
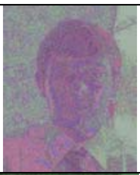
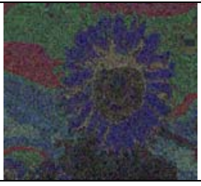
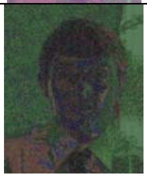
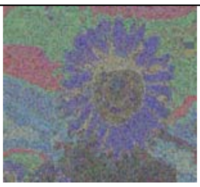
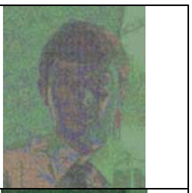
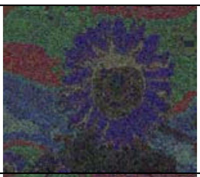
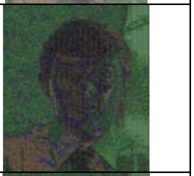
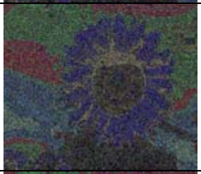
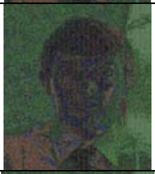
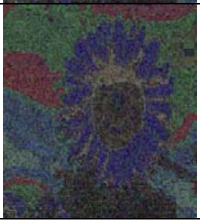
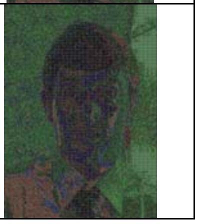
PSNR Of extracted images from the attacked watermarked images
TABLE - I

Our proposed scheme sustained all the attacks and quality of extracted watermark images is also fine. Table-I summarizes the PSNR of extracted image from all test images. We are also showing the recovered images in Table-III. It is clear that recovered images are quite detectible. Table-II shows the recovered images from attacked images.

During our experimentation, we have observed that after applying our algorithm the size of the watermarked image is getting increased. It is happening because of the increase in the number of bytes of the TargetPic as the Passpic is getting watermarked into that. The size can be reduced if we use the Compressed Images or the Portable images that are mostly suitable for the network.

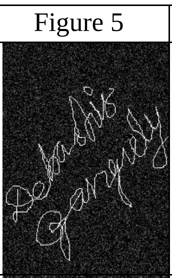
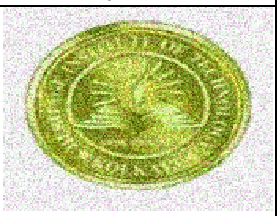
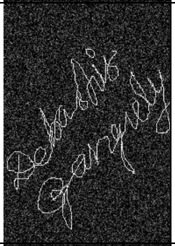
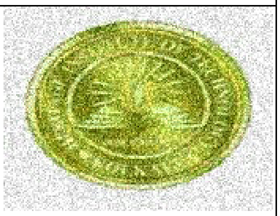
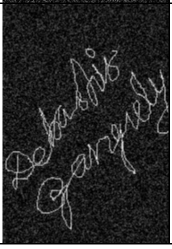
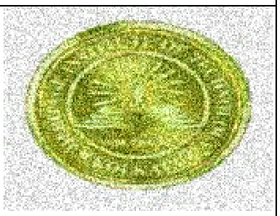
After discussing the entire algorithm, it is quiet clear that the proposed method is more focused on cryptography, i.e., it intends to secure the message over a transport channel. But, we need to understand where lies the novelty of a cryptographic algorithm. A good algorithm is that which can secure the message from any kind of attack if the key is not being compromised considering the fact the algorithm is public. Here, in our case though the encryption is based on the PassPic and we self encrypt it and encrypt the TargetPic with the encrypted key, if an attacker knows the method, he/she can easily frame out its reverse procedure to get the image back having the self-encrypted key. So, it offends the basic need of algorithm being public.

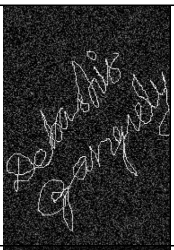
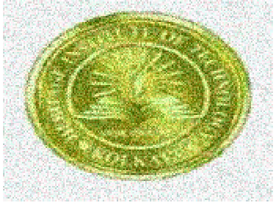
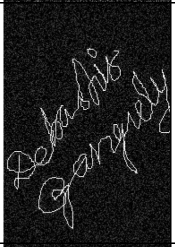
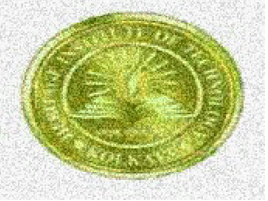
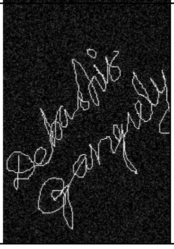
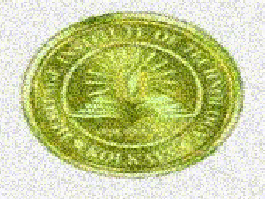
Hence, we can't put it as a cryptographic technique. But, it could stand out in those cases where the algorithm can be proprietary of an individual. For example, we can design a media player which internally implements the decryption logic of our algorithm. So, we can encrypt an audio or video file with a random user specific picture (like: digital signature or company logo which he/she do not share with anyone) and write the encrypted video and algorithm both in the CD/DVD. Then the player when fed by user with his /her secret image can only decrypt that audio/video and play. If the Keypic is supplied wrongly, then only a file containing random noise will be generated. In this way, we can achieve the copyright protection of content between agreed parties. Here, as the algorithm is known to the company only and it obfuscates the need of knowing from user's point. In similar fashion, this algorithm can also be applied to stop the copying of online media contents.

	Figure 3	Figure 8
Attack-1		
Attack-2		
Attack-3		
Attack-4		
Attack-5		
Attack-6		

Watermarked images with different attacks

TABLE – II

	Figure 5	Figure 10
Attack-1		
Attack-2		
Attack-3		

Attack-4		
Attack-5		
Attack-6		

Extracted Target images after different attacks

TABLE - III

V. Conclusion

This watermarking algorithm is supposed to be more efficient as here from the watermarked picture it is difficult to guess the actual size and content of the Target file. And here the watermarked picture is larger in size and blurred in color so it is quite different from the existing watermarking algorithms. Experimental results prove that the proposed scheme is robust against collusion attack as well as common image manipulations procedures and thus it can efficiently be used in the field of Copyright protection both offline and online.

Further research on this work may be conducted on the sustainability of the proposed heuristic against the image compression along with the reduction of extra noise which is getting introduced due to different attacks.

References

[1] M.M. Yeung, et al., “Digital Watermarking for High- Quality Imaging”, In Proc. of IEEE First Workshop on Multimedia Signal Processing, Jun. 1997, Princeton, Page(s): 357-362.

[2] A. M. Eskicioglu and E. J. Delp. “An Overview of Multimedia Content Protection in Consumer Electronics Devices”, Elsevier Signal Processing: Image Communication, Vol. 16, Jan. 2001, Page(s): 681– 699.

[3] Z. Q. Huang and Z. Jiang, “Image Ownership Verification via Private Pattern and Watermarking Wavelet Filters”, In Proc. of VIIth Digital Image Computing: Techniques and Applications, Sun C., Talbot H., Ourselin S. and Adriaansen T. (Eds.), 10-12 Dec. 2003, Sydney, Page(s): 801 - 810.

[4] Anthony T.S. Ho, J. Shen, S.H. Tan and A.C. Kot, “Digital Image-in-Image Watermarking For Copyright Protection Of Satellite Images Using the Fast Hadamard Transform”, In Proc. of IEEE International Geoscience and Remote Sensing Symposium, Vol. 6, 2002, Page(s): 3311– 3313.

[5] Shih-Hao Wang and Yuan-Pei Lin, "Wavelet Tree Quantization for Copyright Protection Watermarking", IEEE Transactions On Image Processing, Vol. 13, No. 2, February 2004, Page(s): 154– 165.

[6] R.J. Hwang, “A Digital Image Copyright Protection Scheme Based on Visual Cryptography”, Tamkang Journal of Science and Engineering, Vol. 3, No. 2, 2000, Page(s): 97– 106.

[7] I.J.Cox, J. Kilian, T. Shamoon, and T. Leighton, “Secure Spread Spectrum Watermarking of Images, Audio and Video”, In Proc. of IEEE International Conf on Image Processing, Vol. 3, Sep. 1996, Switzerland, Page(s): 243–246.

[8] C.-S. Lu, H.-Y. M. Liao, S.-K. Huang, and C.-J. Sze, “Cocktail watermarking on images”, In Proc. of 3rd International Workshop on Information Hiding, Sep. 1999, Germany, Page(s): 333– 347.

[9] Z.-M. Lu, D.-G. Xu, and S.-H. Sun, “Multipurpose image watermarking algorithm based on multistage vector quantization”, IEEE Transactions on Image Processing, Vol. 14, Issue 6, Jun. 2005, Page(s): 822–831.

[10] C.-S. Lu, H.-Y. M. Liao, “Multipurpose Watermarking for Image Authentication and Protection”, IEEE Transactions on Image Processing, Vol. 10, No. 10, Oct. 2001, Page(s): 1579– 1592.

[11] Yongjian Hu and Byeungwoo Jeon, “Reversible Visible Watermarking and Lossless Recovery of Original Images”, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 16, Issue 11, 2006, Page(s): 1423– 1429.

[12] Jengnan Tzeng, Wen-Liang Hwang, and I-Liang Chern, "An Asymmetric Subspace Watermarking Method for Copyright Protection", IEEE Transactions on Signal Processing, Vol. 53, No. 2, Feb. 2005, Page(s): 784– 792.

[13] Ming-Chiang Hu, Der-Chyuan Lou and Ming-Chang Chang, "Dual-wrapped digital watermarking scheme for image copyright protection," Computers & Security, Vol. 26, No. 4, 2007, Page(s): 319– 330.

[14] Shang-Lin Hsieh, I-Ju Tsai, Bin-Yuan Huang and Jh-Jie Jian, "Protecting Copyrights of Color Images using a Watermarking Scheme Based on Secret Sharing and Wavelet Transform", Journal Of Multimedia, Vol. 3, No. 4, Oct. 2008, Page(s): 42– 49.

[15] Kutter, M. and Petitcolas, F. A. P. , “A fair benchmark for image watermarking systems”, In Proceedings of SPIE security and Watermarking of Multimedia Contents, Vol. 3657. Page(s): 226–239.

Swarnendu Mukherjee is currently working in Cognizant Technology Solution, Kolkata, India. His research interest includes Image Processing, Network Security, and Biometric Authentication, Data Mining and etc. He is also a fellow of Computer Society of India and IACSIT. He is a life time member of ACEEE and an active member of IEEE. He has worked as reviewer for different journals and conferences. He has published more than twelve research papers in reputed Journals and IEEE International Conferences.

Debashis Ganguly is a computer science engineer, currently working in the domain of Financial Services and Insurances with Infosys Ltd. He has published more than 20 papers in various international conferences and journals associated with IEEE, Springer and other leading organisations. His research interest includes Image and Digital Signal Processing, Network Security, and Biometric Authentication, Data Mining and related area. He has authored the book “Network and Application Security: Fundamentals and Practices; ISBN 978-1-57808-755-6; Science Publishers, Enfield, New Hampshire and CRC Press, Taylor & Francis Group”. He also plays role of a research reviewer for many international conferences.

Partha Mukherjee has done his bachelors from Jadavpur University and Masters in Computer Sc from Indian Statistical Institute, India and USA. He has over eight years of professional experience in working on technical project consulting, lecturing & research in Computer Science and Engineering. He has serviced major organizations and Institutions in India, and USA. He worked as the consultant in IIT-ISRO project and in Department of Defence (DoD) Project, USA. He has four years of research experience in Computer Sc and Engineering (both in hardware and Software) and has Teaching experience in leading Technical Institutions in Kolkata and West Bengal.

Prasenjit Mitra received his Doctor of Philosophy degree in Electrical Engineering at Stanford University in 2004. He worked under the supervision of Prof. Gio Wiederhold and his dissertation is titled "An Algebraic Framework for the Interoperation of Ontologies". Prior to that, he had received a Master of Science degree in Computer Science at The University of Texas at Austin in December, 1994. His Bachelor of Technology (with Honours) degree in Computer Science and Engineering was from the Indian Institute of Technology, Kharagpur in May, 1993. From 1995, he worked for five years at Oracle Corporation in Redwood Shores, CA as a senior member of the technical staff at the Server Technologies division developing database software. He also worked part-time as a senior engineer at Narus, and DBWizards.