Analysis of Boneh-Shaw Finger Printing Codes under Majority Value Collusion Attacks

Alok Tripathi
IT Division
NIELIT
Patna, India

Rajiv Pandey
IT Department
Amity University
Lucknow, India

ABSTRACT
Lot of research has been done in the previous years to deal with threat of collusion attacks on finger printing codes. Digital fingerprints are code inserted in the media contents before distribution. Each fingerprinting code is assigned to an intended recipient. This fingerprinting code is used to track the culprit in case of illegal distribution of media contents by users. It is now possible for a group of users with different printing codes of the same content to collude together and collectively mount attack against fingerprints. Thus collusion attack poses a real challenge to protect the copyright of digital media. This paper presents an analysis of Boneh-Shaw finger printing codes under Majority Value collusion attacks.

Keywords
Digital Water Marking, Digital Fingerprinting, Collusion Attack, Boneh-Shaw Finger printing Codes

1. INTRODUCTION

1.1 Digital Water Marking
Digital water marking is a technique that enables for the enforcement of the copyright protection of the digital media. It is a technique that is applied to provide security, authentication and copy right protection of the digital media. In digital watermarking a secret message called watermark is embedded inside the digital media. If some problem occurs this secret message is recovered to check the authentication or the real owner of the digital media. The technique is described diagrammatically as follows.

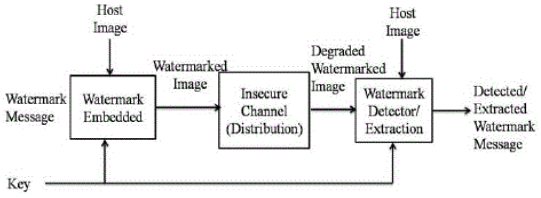

Figure 1. Digital Water Marking

1.2 Digital Finger Printing Codes
In digital fingerprinting unique codes are generated for each digital media file and these unique codes are embedded in their corresponding digital media file. The database mapping of fingerprinting code is done with their corresponding digital files. If after distribution some user makes an illegal copy of its digital media file and redistributes it the illegal copy is traced and the fingerprinting code is extracted. This extracted code is searched in database mapping of fingerprinting codes with digital media file and digital media file is found which is illegally distributed. Now from this database the corresponding user who has distributed the illegal copy is caught. This digital fingerprinting codes help in copyright protection of digital media files. The process is shown diagrammatically as follows:

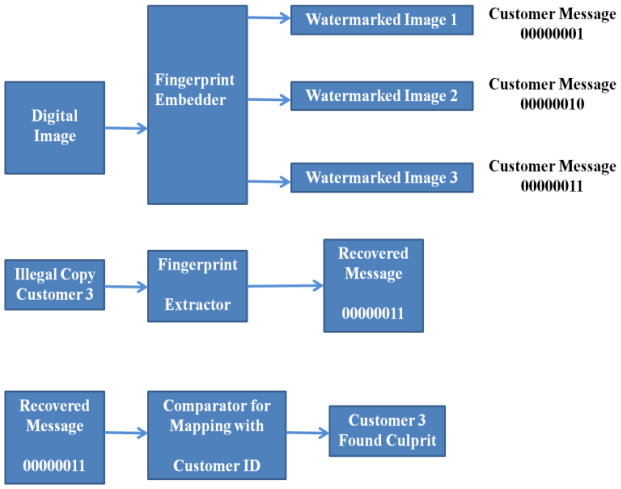

Figure 2. Digital Finger Printing

1.3 Collusion Attack on Digital Fingerprinting Codes
A collusion attack is one in which a group of customers having the illegal copies of same digital media may collaborate and try to manipulate the fingerprints embedded in their data. These users collaborating to generate the manipulated code are known as colluders. These users do the manipulation by comparing their data and then they manipulate the data at the positions where they saw the differences. The UNIX command diff may be used for this purpose. By doing the manipulation the colluders try to generate the digital media copy with destroyed or altered watermark. For e.g. in the diagram the customers 2 and 6 are the colluders and they collaborate to generate a modified media file in such a way that the generated media file contains watermark message allocated to customer 10.

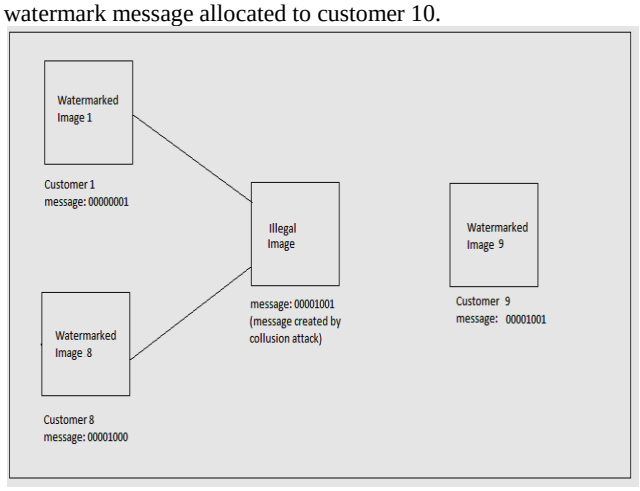

Figure 3. Collusion Attack

1.4 Boneh & Shaw Fingerprinting codes

Boneh & Shaw have tried to solve the problem caused by collusion attack. They have given a secure fingerprinting code that has the length of $O(n^3\log(n/\varepsilon))$ with an ε error rate.

1.4.1 Code Construction

In Boneh & Shaw code for code construction the code constructor will first require the number of users n and the error rate ε, the constructor will generate a code matrix which has n rows and number of columns equal to the length of fingerprinting code. Let Y_m be a column of height n in which the first m bits are 1 and the rest are 0.Let us construct the following matrix

$$Y(n,d)=(Y_1Y_1Y1Y_1)(Y_2Y_2Y_2)\ldots\ (Y_{n-1}Y_{n-1}\ldots\ldots\ldots Y_{n-1})$$

(d times) (d times) (d times)

we define $\Gamma_0(n,d)$ as an (n(d-1),n) code whose code words are the rows of the matrix Y(n,d).The amount of duplication d determines the error probability ε.For e.g. $\Gamma_0(4,3)$ for users A,B,C,D is defined by

$$Y(4,3)=\begin{matrix}1&1&1&1&1&1&1&1&1&A\\0&0&0&1&1&1&1&1&1&B\\0&0&0&0&0&0&1&1&1&C\\0&0&0&0&0&0&0&0&0&D\end{matrix}$$

Before using this code the distributor applies to the columns of Y (n,d) random permutation π. The same permutation π is used for all the users. Let B_m is the set of positions where columns Y_m are mapped by $\pi,|B_m|=d$.In other words if $\pi=(\pi_1,\pi_2\ldots\ldots\ldots\ldots\pi_{dn-1})$ then

$$B_m=\{\pi_1|(m-1)d+1\le 1\le md\}$$

Note that

$\{1,2,\ldots\ldots\ldots d(n-1)\}=B_1\upsilon B_2\upsilon\ldots\ldots\ldots\ldots\ldots\upsilon B_{n-1}$

In fact the permutations of columns of Y(n,d) is defined only by partition of $\{1,2,\ldots\ldots\ldots..,d_{n-1}\}$ in to $B_1,B_2,\ldots\ldots\ldots\ldots B_{n-1}$ because of repetitive columns. Therefore there are only

$$\binom{d(n-1}{d,d,--d}=(d(n-1)!$$

really different permutations of Y(n,d) for $2\le s\le n-1$ define $R_s=B_{s-1}\cup B_s$

For instance suppose for Y(4,3) we use the following permutation

π = (7, 3, 2, 4, 9, 5, 1, 6, 8) then

$$\pi(Y(4,3))=\begin{bmatrix}1&1&1&1&1&1&1&1&1\\1&0&0&1&1&1&0&1&1\\1&0&0&0&0&1&0&1&0\\0&0&0&0&0&0&0&0&0\end{bmatrix}$$

$B_1=\{2,3,7\}$ $B_2=\{4,5,9\}$ $B_3=\{1,6,8\}$

$R_2=\{2,3,4,5,7,9\}$

$R_3=\{1,4,5,6,8,9\}$

1.4.2 Tracing Algorithm for Boneh & Shaw Code

Given $x\varepsilon\{0,1\}^{d(n-1)}$ find a subset of the coalition that produced x.

1. Set all bits to 0
2. If $w(X|B_1) > 0$ then output user 1 is guilty.
3. If $w(X|B_{n-1})$ <d then output user n as guilty
4. For S=2,3,……n-1 do
   Let $k=W(X|R_s)$ if

   $$W(X|B_{s-1}) < k/2-\sqrt{\left(\frac{k}{2}\right)\log n/\varepsilon}$$

   Then output user S is guilty.

1.5 Majority Value Collusion Attacks

In Majority Value collusion attack the colluders compare their codes bit by bit. If codes agree then in the pirated copy the same bit is copied but if the bits of the code disagree then in the pirated copy at that bit position is filled with either 0 or 1 whichever is in Majority at that position in the codes.

2. RELATED WORK

2.1 This paper reviewed the basic model of digital image watermarking for embedding along with some latest research work done on digital image watermarking. Next, it mentioned the requirements of any digital image watermarking System .Then it listed some of the applications of digital image watermarking. Next, it showed the classification based on different categories. Next it highlighted the evaluation system of watermarking technologies by comparing their advantages and disadvantages. Finally it presents some work done on improving watermark as a copyright protection method.

2.2 In this paper it is discussed that Watermarking is most popularly used approach for providing security on images. Under many circumstance watermarking approach is not possible for providing the security. Because of the visibility of the security message, the hackers can create the watermarking on the original image as like the sender sent and then send the modified image to the receiver. Everyone can read the copyright information. To solve the problems in watermarking approach the unique intrinsic fingerprint of the image source coders are taken as the evidence for security. Based on the intrinsic fingerprint of image source encoders, forensic detector is developed. This detector identifies which source encoder is applied, what the coding parameters are along with confidence measures of the result.

2.3 There is various types' watermarks and these have uses and applications. It depends upon which application area one is looking for according to that watermark type is chosen. There are mix and match of techniques, applications and documents on which watermarking are categorized and studied. This paper shows an overview of various kinds of watermark and its implementation area.

2.4 This paper incorporate the detail survey about watermarking, it starts with overview, classification, features, techniques, application, challenges, and limitations of watermarking.

2.5 The large need of networked multimedia system has created the need of "COPYRIGHT PROTECTION". It is very important to protect intellectual properties of digital media. Internet playing an important role of digital data transfer. Digital watermarking is the great solution of the problem of how to protect copyright. This paper emphasizes that Digital watermarking is the solution for the protection of legal rights of digital content owner and customer with the help of fingerprinting.

2.6 Digital watermarking is not a new name in the technology world but there are different techniques in data hiding which are similar to watermarking. In this paper authors compare digital watermarking with other techniques of data hiding. Steganography, Fingerprinting, cryptography and Digital signature techniques are compared with watermarking. They emphasizes that people need water-marking for digital data security .It provides ownership assertion, authentication and integrity verification, usage control and con-tent labeling.

2.7 In this work they show how an existing fingerprint code can be optimized with respect to code length in order to collaborate with a watermarking algorithm to provide a maximum of reliability with a minimum of payload.

2.8 The Internet presents opportunities for individuals to dispatch information in various forms, such as through blogs that are not part of the content distribution routes used by content providers. At the same time, problems must be addressed when copyrighted content is distributed without authorization. To deter these illegal activities, authors say that fingerprinting is attracting attention as a promising content copyrights protection technology.

2.9 Digital fingerprinting protects multimedia content from illegal redistribution by uniquely marking copies of the content distributed to users. Most existing multimedia fingerprinting schemes consider a user set on the scale of thousands. However, in such real-world applications as video-on-demand distribution, the number of potential users can be as many as 10–100 million. This large user size demands not only strong collusion resistance but also high efficiency in fingerprint construction, and detection, which makes most existing schemes incapable of being applied to these applications. A recently proposed joint coding and embedding fingerprinting framework provides a promising balance between collusion resistance, efficient construction, and detection, but several issues remain unsolved for applications involving a large group of users. In this paper, authors explore how to employ the joint coding and embedding framework and develop practical algorithms to fingerprint video in such challenging settings as to accommodate more than ten million users and resist hundreds of users' collusion. They investigate the proper code structure for large-scale fingerprinting and propose a trimming detection technique that can reduce the decoding computational complexity by more than three orders of magnitude at the cost of less than 0.5% loss in detection probability under moderate to high watermark-to-noise ratios. Both analytic and experimental results show a high potential of joint coding and embedding to meet the needs of real-world large-scale fingerprinting applications.

2.10 With a digital fingerprinting scheme a vendor of digital copies of copyrighted material marks each individual copy with a unique fingerprint. If an illegal copy appears, it can be traced back to one or more guilty pirates, due to this fingerprint. Boneh and Shaw [18] have devised a classic fingerprinting scheme, and several recent papers have designed improvements. In the present paper authors make a new error analysis of Boneh and Shaw's original scheme,[18] and they prove that it is far better than assumed and in fact better than the improvements in some respects.

2.11 Authors have shown that an efficient collusion-secure code with error-correction can be built based on the Boneh-Shaw code [18]. The error-correction helps to build a complete watermarking/fingerprinting scheme resistant to attacks on the watermarking layer. They show that impact of errors on the information rate is surprisingly low.

2.12 The work presented in this paper consists in the development of a portable platform to protect the copyright and distribution rights of digital contents, and empirically demonstrate the capacity of several marking and tracing algorithms. This platform is used to verify, at a practical level, the strength properties of digital watermarking and fingerprinting marks. Initially, two watermarking algorithms, one based on spread-spectrum techniques and the other based on QIM (Quantization Index Modulation), have been implemented. Moreover, authors use these watermarking algorithms to embed a fingerprinting code, based on code concatenation, equipped with an efficient tracing algorithm. In this paper they focus on the implementation issues of the Java based platform that consists of three main packages that are fully described.

2.13 A pirate is a person who buys a legal copy of a copyrighted work and who reproduces it to sell illegal copies. Artists and authors are worried as they do not get the income which is legally theirs. It has been suggested to mark every copy sold with a unique fingerprint, so that any unauthorized copy may be traced back to the source and the pirate who bought it. The fingerprint must be embedded in such a way that it cannot be destroyed. Two pirates, who cooperate, can compare their copies and they will and some bits which differ. These bits must be part of the fingerprint, and when the pirates can see and change these bits, they get an illegal copy with neither of their fingerprints. Collusion secure fingerprinting schemes are designed to trace at least one of the pirates in such collusion. In this paper authors prove that so called (2, 2)-separating codes often are collusion-secure against two pirates. In particular, they consider the best known explicit asymptotic construction of such codes, and prove that it is collusion-secure with better rate than any previously known constructions.

2.14 Collusion-secure fingerprinting codes are an important primitive used by many digital watermarking schemes. Boneh and Shaw [18] define a model for these types of codes and present an explicit construction. Boneh and Shaw [18] also present a lower bound on the length of any collusion-secure code. Authors give new lower bounds on the length of collusion-secure codes by analyzing a weighted coin-flipping strategy for the coalition. As an illustration of their methods, they give a simple proof that the Boneh- Shaw [18] construction cannot be asymptotically improved. Next, they prove a general lower bound.

2.15 A construction is presented to obtain 3-secure fingerprinting codes for copyright protection. Resistance against collusions of up to three buyers is achieved with a code word length dramatically shorter than the one required by the general Boneh-Shaw construction [18]. Thus the proposed fingerprints require much less embedding capacity. Due to their very clandestine nature, collusions tend to involve a small number of buyers, so that there is plenty of use for codes providing cost-effective protection against collusions of size up to 3.

2.16 Authors examine the problem of Collusion-Secure Fingerprinting in the case when marks are binary and coalitions are of size 2. They are motivated by two considerations, the pirates' probability of success (which must be non-zero, as was shown by Boneh and Shaw [18]) on one hand, and decoding complexity on the other. They show how

to minimize the pirates' probability of success: but the associated decoding complexity is O(M 2), where M is the number of users. Next they analyze the Boneh and Shaw [18] replication strategy which features a higher probability of success for the pirates but a lower decoding complexity. There are two variations. In the case when the fingerprinting code is linear they show that the best codes are linear intersecting codes and that the decoding complexity drops to O(log2 M). In the case when the fingerprinting code is allowed to be nonlinear, finding the best code amounts to finding the largest B 2-sequence of binary vectors, an old combinatorial problem. In that case decoding complexity is intermediate, namely O(M).

2.17 Electronic copyright protection is increasingly dependent on fingerprinting and watermarking techniques. In this paper the properties of dual binary Hamming codes are exploited to obtain a fingerprinting scheme secure against collusion of two buyers. The advantage over previous proposals is that collusion security is obtained using well-known and shorter length error correcting codes.

2.18 This paper discusses methods for assigning code words for the purpose of fingerprinting digital data, e.g., software, documents, music, and video. Fingerprinting consists of uniquely marking and registering each copy of the data. This marking allows a distributor to detect any unauthorized copy and trace it back to the user. This threat of detection will deter users from releasing unauthorized copies. A problem arises when users collude: for digital data, two different fingerprinted objects can be compared and the differences between them detected. Hence, a set of users can collude to detect the location of the fingerprint. They can then alter the fingerprint to mask their identities. Authors present a general fingerprinting solution which is secure in the context of collusion. In addition, they discuss methods for distributing fingerprinted data.

2.19 This white paper provides a high level overview of digital watermarking and fingerprinting and examines how these two technologies can be integrated into workflows for automatically tracking, protecting and monetizing content.

2.20 This Paper examines some early examples of steganography and the general principles behind its usage. It then looks at why it has become such an important issue in recent years. Then there is a discussion of some specific techniques for hiding information in a variety of files and the attacks that may be used to bypass steganography.

This paper analyses the Boneh & Shaw code under Majority value collusion attack. The analysis is done using a simulator coded in Java. The experimental results are presented and detailed analysis of performance of Boneh& Shaw code under majority Value collusion attack is shown.

3. PROPOSED WORK

The work done has been summarized as follows

- Construction of Boneh& Shaw code has been simulated by developing a simulator in Java
- Accusation algorithm of Boneh& Shaw code has been simulated by developing a simulator in Java.
- Majority Value collusion attack has been simulated by developing a simulator in Java.
- Accusation algorithm simulated using Java has been used to detect the pirates who have colluded to launch the attack.

The comparison of present work with exiting works is as follows:

a) Practical Simulation of Construction of finger printing codes (Boneh & Shaw) has been performed.

b) The Collusion attack (Majority Collusion Attack) has been launched practically on finger printing codes constructed in step (i).

c) The Accusation algorithm (Boneh & Shaw code) has been practically implemented to detect the colluders who have performed the collusion attack in step (ii).

d) The analysis has been performed by using different combination of colluders, different collusion sizes, different coding lengths; different error rate, different number of users practically and results have been summarized in experimental result section.

e) The present work practically analyses the performance of Boneh& Shaw code under majority value collusion attack by creating different scenarios of different colluders, different collusion sizes, different coding lengths, different number of users & different error rate.

Thus this paper serves as a base for practically analyzing the Boneh & Shaw code with attacks other than majority value Collusion attacks and compare with the results obtained here.

4. EXPERIMENTAL RESULTS

The following experimental results have been deduced after performing the above proposed work. The evaluation has been shown for 40 users.

Table-1. Experimental results at 1% error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	10	834210	0
40	3	10	834210	0
40	5	10	834210	0
40	10	10	834210	0
40	15	10	834210	0
40	20	10	834210	0
40	25	10	834210	0

Table-2. Experimental results at 5% error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	5	920712	0
40	3	5	920712	0
40	5	5	920712	0
40	10	5	920712	0
40	15	5	920712	0
40	20	5	920712	0
40	25	5	920712	0

Table-3. Experimental results at 10% error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	10	834210	0
40	3	10	834210	0
40	5	10	834210	0
40	10	10	834210	0
40	15	10	834210	0
40	20	10	834210	0
40	25	10	834210	0

Table-4. Experimental results at 15 % error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	15	783627	0
40	3	15	783627	0
40	5	15	783627	0
40	10	15	783627	0
40	15	15	783627	0
40	20	15	783627	0
40	25	15	783627	0

Table-5. Experimental results at 20 % error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	20	747708	0
40	3	20	747708	0
40	5	20	747708	0
40	10	20	747708	0
40	15	20	747708	0
40	20	20	747708	0
40	25	20	747708	0

Table –6. Experimental results at 25 % error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	25	719862	0
40	3	25	719862	0
40	5	25	719862	0
40	10	25	719862	0
40	15	25	719862	0
40	20	25	719862	0
40	25	25	719862	0

Table –7. Experimental results at 30% error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	30	697125	0
40	3	30	697125	0
40	5	30	697125	0
40	10	30	697125	0
40	15	30	697125	0
40	20	30	697125	0
40	25	30	697125	0

Table –8. Experimental results at 35 % error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	35	677859	0
40	3	35	677859	0
40	5	35	677859	0
40	10	35	677859	0
40	15	35	677859	0
40	20	35	677859	0
40	25	35	677859	0

Table –9. Experimental results at 40 % error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	40	661206	0
40	3	40	661206	0
40	5	40	661206	0
40	10	40	661206	0
40	15	40	661206	0
40	20	40	661206	0
40	25	40	661206	0

Table-10. Experimental results at 45 % error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	45	646503	0
40	3	45	646503	0
40	5	45	646503	0
40	10	45	646503	0
40	15	45	646503	0
40	20	45	646503	0
40	25	45	646503	0

Table 11. Experimental results at 50 % error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	50	633360	0
40	3	50	633360	0
40	5	50	633360	0
40	10	50	633360	0
40	15	50	633360	0
40	20	50	633360	0
40	25	50	633360	0

Table-12. Experimental results at 60% error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	60	610623	0
40	3	60	610623	0
40	5	60	610623	0
40	10	60	610623	0
40	15	60	610623	0
40	20	60	610623	0
40	25	60	610623	0

Table –13. Experimental results at 70% error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	70	591357	0
40	3	70	591357	0
40	5	70	591357	0
40	10	70	591357	0
40	15	70	591357	0
40	20	70	591357	0
40	25	70	591357	0

Table-14. Experimental results at 80% error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	80	574704	0
40	3	80	574704	0
40	5	80	574704	0
40	10	80	574704	0
40	15	80	574704	0
40	20	80	574704	0
40	25	80	574704	0

Table-15. Experimental results at 90% error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	90	560001	0
40	3	90	560001	0
40	5	90	560001	0
40	10	90	560001	0
40	15	90	560001	0
40	20	90	560001	0
40	25	90	560001	0

Table-16. Experimental results at 95% error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	95	553254	0
40	3	95	553254	0
40	5	95	553254	0
40	10	95	553254	0
40	15	95	553254	0
40	20	95	553254	0
40	25	95	553254	0

Table-17. Experimental results at 99 % error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	99	548106	0
40	3	99	548106	0
40	5	99	548106	0
40	10	99	548106	0
40	15	99	548106	0
40	20	99	548106	0
40	25	99	548106	0

Table-18. Experimental results at 100% error rate

No of Users	Size of Collusion	Error rate %	Length of Finger Printing Codes	% of False Positive
40	2	100	546858	0
40	3	100	546858	0
40	5	100	546858	0
40	10	100	546858	0
40	15	100	546858	0
40	20	100	546858	0
40	25	100	546858	0

Also it has been observed that as the number of users increases Java Starts showing heap space error. The solution to above problem is that powerful servers of high configuration should be deployed for using Boneh& Shaw code for fingerprinting for copyright protection with practical applications also with very large users we may require supercomputers for using Boneh & Shaw code for practical applications.

Also from simulation results it is observed that for Boneh & Shaw code implementation the number of users should be known at the beginning of implementation it is not possible to dynamically add users.

From the simulation results it is observed that no false positives are there for Boneh & Shaw code even at error 1 hence Boneh & Shaw code is foolproof against the random bit collusion attack.

It is observed while performing experiments that under Majority Value attack accusation algorithm always accuses one pirate because the anatomy of majority value attack is such that the pirated copy matches one of the fingerprinted copies.

The next observation is that accusation algorithm never accuses user 1 because the pirated copy produced by majority attack never matches user 1.This is clear from anatomy of majority value attack that all the bits in the pirated copy could not be one. This observation has been validated by experimental results while performing the experiments.

5. CONCLUSION

From the simulation performed in this paper it is clear that Boneh & Shaw code are foolproof against the majority value collusion attacks. Also powerful servers should be deployed for practical application of Boneh & Shaw code. The number of users should be known in advance for practical application of Boneh & Shaw code. Also our next effort will be to simulate Boneh & Shaw code with more attack like Binary Addition attack and compare the results obtained with this work.

6. REFERENCES

[1] S Sahar Afshan Andrabi, Sheenam. A Review: Information Hiding Using Watermarking Techniques. SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE) – EFES April 2015.

[2] V A. Sudha, K. Vanitha, A. NooralShaba. Efficient Analysis And Secure Client Side Image Using Fingerprint Embedding International Journal of Scientific & technology Research Volume 3, Issue 1, January 2014 ISSN 2277-8616.

[3] Sharbani Bhattacharya et al. Survey on Digital Watermarking – A Digital Forensics & Security Application International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 11, November 2014.

[4] Kusuma Kumari A Survey of Digital Watermarking Techniques and it Applications Karnataka, India International Journal of Science and Research (IJSR)ISSN (Online): 2319-7064 Volume 2 Issue 12, December 2013.

[5] Miss. Nupoor M. Yawale1, Prof. V. B. Gadicha2. Digital Watermarking and fingerprinting:A good idea for security. International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 2, Issue 2, February 2013 ISSN 2319 – 4847.

[6] Gurpreet Kaur, Kamaljeet Kaur Digital Watermarking and Other Data Hiding Techniques International Journal of Innovative Technology and Exploring Engineering

(IJITEE) ISSN: 2278-3075, Volume-2, Issue-5, April 2013.

[7] Marcel Schäfer, Waldemar Berchtold, Margareta Heilmann, Sascha Zmudzinski, Martin Steinebach, Stefan Katzenbeisser. Collusion Secure Fingerprint Watermarking for Real World Applications Proc. of GI-Sicherheit 2010.

[8] Satoshi Fujitsu. Fingerprinting. Broadcasting Systems. Series: Challenges: "Information Security Technology in the Digital ... Broadcast Technology No.36, Spring 2009. NHK STRL. C. 21. Challenge. CAS technology overview. Broadcasting.

[9] Shan He and Min Wu. Collusion-Resistant Video Fingerprinting for Large User Group. IEEE Transactions on Information Forensics and Security, Vol. 2, No. 4, December 2007.

[10] Hans Georg Schaathun. The Boneh–Shaw Fingerprinting Scheme is Better Than We Thought. IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, JUNE 2006.

[11] Schaathun, H.G. . On watermarking/fingerprinting for copyright protection. Proceedings of the 1st International Conference on Innovative Computing, Information and Control, Volume 3, August 30-September 1, 2006, Beijing, China, pp: 50-53.

[12] Miguel Soriano, Marcel Fernandez, Elisa Sayrol, Joan Tomas,Joan Casanellas,Josep Pegueroles, and Juan Hernández-Serrano. Multimedia Copyright Protection Platform Demonstrator. P. Herrmann et al. (Eds.): iTrust 2005, LNCS 3477, pp. 411-414, 2005.

[13] Hans Georg Schaathun. Fighting two pirates. Chapter Applied Algebra, Algebraic Algorithms and Error-Correcting Codes Volume 2643 of the series Lecture Notes in Computer Science pp 71-78, April 2003.

[14] Chris Peikert abhi shelat Adam Smith. Lower Bounds for Collusion-Secure Fingerprinting. Proceeding SODA '03 Proceedings of the fourteenth annual ACM-SIAM symposium on Discrete algorithms Pages 472-479,2003.

[15] Francesc Seb´e and Josep Domingo-Ferrer. Short 3-Secure Fingerprinting Codes for Copyright Protection.Chapter Information Security and Privacy Volume 2384 of the series Lecture Notes in Computer Science pp 316-327 , 2002.

[16] Gérard Cohen, Simon Litsyn, Gilles Zémor. Binary Codes for Collusion-Secure Fingerprinting Inforrmation Security and Cryptology — ICISC 2001Volume 2288 of the series Lecture Notes in Computer Science pp 178-185 Date: 23 April 2002.

[17] J. Domingo-Ferrer and J. Herrera-Joancomarti. Short collusion-secure fingerprints based on dual binary Hamming codes. Electronics Letters 28th September 2000 Vol. 36 No. 20.

[18] Dan Boneh and James Shaw .Collusion-Secure Fingerprinting for Digital Data. IEEE Transactions on Information Theory, Vol. 44, N0. 5, September 1998.

[19] Content Control: Digital Watermarking and Fingerprinting by Dominic Milano Rhozet http://www.carbonserver.com/whitepapers/Fingerprinting_Watermarking.pdf.

[20] Steganography And Digital Watermark http://www.gnu.org/copyleft/fdl.html

7. AUTHOR PROFILE

Mr Alok Tripathi Member IEEE is Director-in-Charge at NIELIT Patna, Bihar, India. He possesses a diverse back ground experience of around 20 years of Academic experience. His research interests include the contemporary technologies as Information Security, Cloud computing and Database systems. He has been on technical Committees of Various Government and Private Universities. He is intellectually involved in supervising Post graduate Students. He has been the Principal Investigator of 3 National Level Information Security Projects.

Dr. Rajiv Pandey Senior Member IEEE is a Faculty at Amity Institute of Information Technology, Amity University, Uttar Pradesh, Lucknow Campus, India. He possesses a diverse back ground experience of around 30 years to include 15 years of Industry and 15 years of academic. His research interests include the contemporary technologies as Semantic Web Provenance, Cloud computing, Big-Data, and Data Analytics. He has been on technical Committees of Various Government and Private Universities. He is intellectually involved in supervising Doctorate Research Scholars and Post graduate Students. He is also an active contributor in professional bodies like IEEE, IET and LMA. He is a member of Machine Intelligence Labs.