

Unified Model for Fingerprinting Code Applications

Ibrahim Nasir Aliyu*

Computer Engineering Department, Hussani Adamu Federal Polytechnic Kazaure, Jiagawa State.

ABSTRACT

The enormous popularity of digital contents contains unlicensed and illegal activity which are involved in different perspectives. Despite several efforts are made toward an illegal copy and redistribution (legal and technical), still the problems exist with growing use of digital application such as storing and distribution of contents, the problem is becoming more worrisome. Attaching a unique invisible marking to every unit of object, is viable trading with problems of unauthorised copying, that is if an illegal copy is released elsewhere, it is going to be practical to find the original owner of the object (traitor). This phenomenon of enforcement, in a copyright protection, is what is referred to as fingerprint code. Dealing with code, for fingerprinting in a digital contents, in the context of several users combining (colluding) to create a new, unauthorised copy (pirate). Theoretical bounds on the performance in the code are realised, with general methods of theoretically observe whether certain users are involved in the illegal activity (copy and redistribution) is presented, and the pirate strategies are identified. A group of users should be considered guilty of been able to create a new compromised contents, when a method's is observe and tracing to identify one of the traitor found in a number of colliding pirates by the use of checkmate items features.

Keywords: Fingerprint code, Traitor, Pirate, Broadcast

1 INTRODUCTION

The development of information in today's digital world, is configured in to the multimedia content for easy access, to pertinent information, for instance; Audio, Images, videos etc. And be sufficiently available. Despite the numerous advantages it provided, with the enormous growth, in the usage of digital means of storing and distributions. It is posed with detrimental challenges, to ensure the reliable and efficient contents. It is indeed important to find a safest mechanism to enhances a fruitful business, that is taking place in a digital networks, and the intended contents are used by authorised users, who have the right for the access of such contents appropriately. In spite of the fact, the administrating to access of the contents, it is quite a significant element to make sure the content is used mainly for the receiver (authorised user). It is however, not enough for the protection of the content integrity. Some of the content protections such as encryption mechanism ceases to be sighted, if the stored contents ceases to be in the encryption domain. And this is seriously affect the owner of original content distributor. The dubious act of unauthorised copy is a threat to various aspect as per as digital productions is concern. These contents of the

data are copied illegally all over the world, as such the original owner of the product suffer Lots in loosing by what it is caused. Initially, the illegal activities was under moderate control by the law enforcement agencies, to deal with redistribution problems and the fact that copies usually have a lower quality then the original, but due to the advancement of Internet technology and digital buffered data , the tune has changed, it makes such illegal copying so easy and cheap to the users in the Internet community. Knowing such illegal activity is taking place with minimum effectual hindrance to deter, only by making the risk of caught quite greater and the only by way this could be achieved is by usage of fingerprint code technology (schemes). The rationale behind the fingerprint code is that each user will receive a copy of the content data attached with a unique mark. The marking will serve to identify the uniquely content data and the particular user if his identity is linked to that data in anyway.

Providing the defensive mechanism, in fighting against the illegal activity toward the digital contents (piracy) is "Traitor Tracing", where by the user who involved in the illegal activity is referred as a "traitor",

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

and is traced back, whenever the illegal copy is identified by the tracer (distributor/owner). Traitor tracing is a technique used, in finding the possible culprit, who have unfaithfully responsible for the emergence of a newly compromised copy of a digital content, and redistribute it illegally. A user who is found guilty, of such illegal act is apprehend or in the situation where by the traitors colludes with the intention of comparing their authorised legal copy and able to produce illegal copy are referred to as "Pirates". And those that are using such illegal copied contents are prominently called pirate users. These pirates' breaches the security of the privileges provided to them, with the intention of accessing a legal copy, and allowed the bad users (unauthorised) to have an illegal access. This process of traitor tracing, uses a very important handy mathematical tool, for a design of robust technique called "Fingerprint code", in achieving the fight against the traitors.

Fingerprint code is an indicator of unique marking to each distributed digital contents, that can possibly takes various forms, depending on the context of the contents. There are actually, various models, in which the fingerprint code is quite applicable in traitor tracing phenomena, that will be discuss in application area of this work. However, these models will be realistic in preparation with the anticipation that illegal copy and redistribution is always in the frontline occurrence, and a good determination measures shall always be focused. It assumes, a good countermeasures will be able to meet certain expectation below;

- I- The capability of the scheme to track the initiation of the illegal activity (piracy).
- II- The pirate users should be revoke from the list of innocent users
- III- The innocent users shall not be distracted/harm.
- IV- The tracing techniques should be able to provide concrete evidence that, the identity of the pirate is purely distinguished. Thus, fingerprinting technique comprises the initial establishment of fingerprint code, secondly the process of attaching the marks, thirdly identification of compromised copy and traceability.

Today, research schemes in the field of information technology have came up with several fingerprinting techniques notably with its numerous significances, especially in the collusion secured fingerprint; where

a unique generated code (set of codeword's) are applied in to each of the user's copy. And can lead the tracer to identify at least one of the responsible user, in case, the content is manipulated under collusion attack and being distributed illegally. But lack of the comprehensively unified literature survey, on the applicable areas, where these phenomenal techniques are materialised and a new shorter way other then classically motivated approach. That is what this work intended to focus on.

This research work will focus on a survey on traitor tracing techniques, in which the fingerprinting codes on digital contents is applicable by identifying a shorter efficient way, that satisfy the properties of identification capabilities in traitor tracing to check mate the illicit usage of digital contents.

1.1 Fingerprint Ideology Concepts

In trying to deter people from illegal digital activities; the scenario could be achieved in one of the ways is by making the punishment for those caught. On the other hand is by technical (schematic) means, in which the "fingerprint" employed. The rationale behind the fingerprint is to mark each copy uniquely, so that every distributed copy is differentiated from each other, by doing so, it is possible to distinguishes between the copies. Thus, if the distributed copy copies only to person (legal) who identify themselves, it might be possible if an illegal copy is found, to identify the person who has the legal copy from which the illegal copy was made. After identifications, it is hope to deter the users from trying the illegal acts, since after they leak the illegal copy they no more have control over it and could possibly be traced and be identified and be prosecuted for such act. So the risk of been identified ought to make it less popular to engage in spread of illegal copies (compromised).

Fingerprint code has to be in such away that, it is not possible to be visualised to any user and could not remove it, else tried it; the fingerprint has a unique properties that if the object is copied, the fingerprint code will be also be copied so that the new copy contain same previous fingerprint code as the

original copy. It is quite interesting, but trivial in putting a fingerprint code where it does not affect the data, for instance in text documents, by coding a fingerprint as small alteration in the space between the letter or rows. This is bad because by copying only the interesting data, it is possible to remove the markings.

In the text document case is just by retyping the whole text document which may be tedious but possible, the solution is to put marking in the data that forms the products. The most interesting part is the way of marking fingerprint (encoding digit individually by marking alteration in the object) is what distinguishes the fingerprint problem in to units which can be properly treated; the embedding and coding problem. The embedding is a way to make the alteration by encoding single digit in to the contents while the coding is how to choose the fingerprint in their abstract representation (vector of digit) as such the fingerprint will be robust against different form of attacks.

1.2 Fingerprint Goals

Some of the targeted goals expected to achieved in fingerprinting is; (1) Ability to provide distinct copies of content. (2) When traced, the scheme should be able to identify the traitor (s)/pirate (s) users and as many as possible. (3) The scheme should be able to observe and revoke several group of users who are guilty of creating compromised copy. (4) Ability to fits various forms in a digital context. In these cases, first is receiving the fingerprint code of the illegal copy and used the black-box to observe the situation by running of some identification algorithm.

2 Discussion on Related areas

Some of the related area to be describe and referenced could not be considered as a whole but a mere considering a bigger picture of further reading and how this work encompass in widened the horizon, considering the work of hurting and kutler 1990 and new edited version by ketzenbeisser and pititcolas [?] in fingerprinting, watermarking and stenography.

2.1 Stenography

the stenography is a scheme in which the message is embedded with hidden information, the embedded can be parametrized by a key that is used when retrieving the hidden information. The secrete message may also be encrypted for the purpose of additional security, but they are two different schemes. In general with several further references conducted by anderson and petitcolas [5]. A theoretical analysis of stenography have been presented by ettinger [6]. The practical bound of stenography by Adam strizel [7], uses the embedding of secrete message (hiddentext), seemingly innocuous objects (coverttext) to produce

a stegotext. When the receiver of the messages (stegotext), obtained a copy then he uses the known techniques employed from the stenography for the successful recovery of the hidden messages. Actually, the main aim of stenography is to communicate between parties in a disguise manners, so that the unintended third party cannot understand what are the actual meaning of the message in a whole communication. It is not exactly like cryptographic (secrete) form, despite the fact that, it provide a very private communication which is so difficult for the attacker to navigate and extract the meaningful information.

2.2 Watermarking

Digital watermarking is another viable method for the protection of ownership, right of digital audio, images, Video. It can be applied to different application include copy protection, device controls, broadcast monitoring fingerprinting, proof of ownership. It is much like stenography only that the schemes should be robust against active attackers, even if they know not only that an object contain watermark, but also if they know the algorithm principle of the method. The proposed application for watermarking is usually copyright information/validation. In [10], by hurting and kutters there is computer application of watermarking and several concept papers on watermarking could be found on communication of the ACM [11]. Recent techniques with cryptographic protocol by minouru Kuribayashi [12] elaborated the significance of implementations spread spectrum watermarking on encrypted domain. And conventional methods by kuribayashi and Tanaka [12]. The trace and Revoking pirate rebroadcasting explained and analysed by Aggelos kiayias and Serdar pehlivanoglu [3]. This security called Watermarking has important dual portions of stage, One is the embedding stages and the other is detection stage. From these two stages, the former is the stage when the watermarking is integrated in to the content of the data, to prevent changes in the content of that particular data. While the detection stage is the one that, the embedded watermarked content can be identified using the secrete key, used at embedding stage, only known to the authorised user. The expected qualities derives and exhibit by the good watermarking technique, includes; 1.Security- The watermark should be able to secure the content of digital data, by not allowing the attacker to make any form of attack on the digitally multi- media content,

and he could not possibly know/find the secret key, even if he knew the algorithm used in the technical processes. 2 Robustness- The watermark is going to be robust, if the content of the multi-media data is modified and yet, the quality is identified to scale through, for the instance in conversion and compressions of data. 3. Capacity- When the content of the data is capable of allowing the several integration of watermark to same content, so as to enforce the detection of reliable content. All in the process of watermarking, it is quite important to note with differencelessness in the content in terms of qualities of any forms such as visual, Audio etc. By the fully technique for the establishment of watermarks, a copy right enforcement measures has been ordained, in digital contents and tracing capabilities. This provides a comprehensive defence mechanism for digitally embedded watermarks in to content (image), as such detection and readability is addressed, largely linking to the detail information about the owner/distributor for right to license.[13],[14].

2.3 Understanding some terms

Understanding these parameters will help in the better significances on the subject matters; I- Partition; is a user set in the collection of subdivision, equivalent to disjoint set of codewords. Partitions in every subset contain one finite block cell. II- Attributes (disjoint); is an index subset features of singleton in the user set of a block partition. III- An Object can be best understood as a collection of digitally stored data such as texts, images, videos, and Audio. When an object is referred as same working purpose for usage, this could be having different meaning for different people and depend on what the object is used for. IV- Illegal Distributions; all forms of distributions to other than by a rightful distributors is considered as unwanted and should not be practice but due a certain users, they leak the contents to authorised personnel's, these users are called traitors. V- Pirates are users performing illegal distribution. Number of pirate c and the set of pirate is denoted $P = P_1, P_2, \dots, P_c$, if P contain more than one pirate is called collusion cooperation. The pirates will distribute to a person other than the user who wants a copy, this is prohibited and to discourage the distributor should use fingerprinting. VI- A collusion is the coming together (cooperation) to work in a purpose of producing an illegal copy of a fingerprinted object. The set of marks are what

consisted in the binary form for the fingerprints code, which is denoted by 0, 1. In coming together of the pirates, they can detect their difference in the means in the marks in between of their copies, else the marks are undetectable. A detectable marks can be change to any of the state, for example 0, 1, ?, in which the marks '?' is invisible and can never be understood which is it, among '0's and '1's. It is noticeable assumptions in the marks that satisfying these sort of property exist for the object being fingerprinted. Note that a situation where by no collusion fingerprinting is trivial by the marking assumption, the fingerprinting allocated to a pirate will be visible (readable) in any illegal copy he distributed.

2.4 Definitions.

A codeword is a sequence of marks that are placed in content. And fingerprint is the assembling of marks. A fingerprint can be understood as a term of length l over an alphabetic size q , where l is number of placed marks. Given an (l, n, q) -code C , each codeword $x \in C$ is considered as a unique fingerprint of a receiver that has access to an object/functionality through its codeword. We, further, suppose that any codeword in Q_l would also be useful in accessing the same object/functionality. In an application where the above assumption holds, an adversary (we will call pirate) is modelled as corrupting a number of receivers (we will call traitor) and retrieving their codeword's. The pirate then runs a Forging algorithm that produces a pirate codeword in $p \in Q_l$. In any reasonable setting, the Forging algorithm is contingent to a marking assumption which enforces the pirate to produce a codeword that is possible according to what the pirate has corrupted. More formally, we define the marking assumption as follows;

Marking assumption; in a fingerprinting where an individual codeword is assign to the users set over an alphabetic size. Every user is obtained a copy of content with the marks that are assign according to his codeword. When users collude, they can find the difference of the marks in between their codewords (forging strategy), and can produce a new pirated copy. but the aimed property of the marks is that the user of the object cannot make any alteration on the object content, if they cannot find the marks in the object in which subsequently makes it useless and these property leads to what is known to be a "Marking Assumption"

If the set of traitor in the number of users, and for all set of codeword $C = \{c_1, \dots, c_n\}$ where a c_j is an element that is contain in a length l of an alphabetic size Q , for which j is an element in the number of users set. It hold that forging algorithm yields a codeword P out (descendant) of the valid user's codeword's $CT = \{c_j \mid j \in T\}$ which is the element of codeword's contain in a traitor codeword's. The descendant set is denoted by $\text{desc desc}(CT)$, and defined as; $\text{desc}(CT)$ is equivalent to a fingerprint code in a number of users with a fingerprint a_i over a length l of alphabetic size Q , found as an element in the traitor coalition, as such a colluding traitors with compromised copy is possibly link back to atleast one traitor involved in the collusion. It is in high probability that the traitor will be traced back among the coalition members and will not overshoot the number of legal users.

$\text{desc}(CT) = \{x \in Q^l : x_i \in \{a_i : a \in CT\}, 1 \leq i \leq l\}$ where x_i, a_i are the i -th symbol of the related vectors. CodeGen: is the code generating algorithm that input l_n and a pair of typical (C, tk) sample; where in the sample, C is an (l, n, q) -code that is defined over an alphabetic Q and l as a function of (n, q) and identifying key tk as an auxiliary information be used for identification (which may be empty).

Identify: is the second algorithm (deterministic) that is been employed after codeGen, takes input a pair sample (C, tk) where C is an element contained in an alphabetic size with a length l , and the tk as an identification key, which yielded result to a codeword found in the number of traitors or the algorithm fails to identify. This fingerprinting code is referred as open, if tk is empty.

The fingerprinting code is define as (codeGen, Identify) and this pair of algorithm is also denoted as (α, ω) -identifier, in a condition on an event A , if the following condition holds;

- I- CodeGen with given input l_n is resulted in producing identification key tk and (l, n, q) -code $C = (C_1 \dots C_n)$. This satisfy the conditional event A .
- II- For any forging algorithm that satisfies the marking assumption, it hold that; For every traitor contained in a number of users, such that the number of traitors is less than or equal to ω . The probability of not identifying (tk, P) contained in the number of traitor will be greater than equal to α , where the pirated copy over an alphabetic size

q is the result of forging algorithm in corresponding to the input $CT = \{c_j \mid j \in T\}$.

3 Fingerprinting Application

3.1 Watermarking

In the consideration of an important business transaction and distribution medium of digital content, on the Internet is pretty much excellent, however a serious issue is possible ways to counter numerous copyright violation and management. This has put the security of digital content to a high profile at stake. Today, the digital images can be found and used everywhere with permission or not. And this usage without permission because a detriment to the market performance by the owner [17]. The innovative technique towards securing of digital content has proudly became a major concern in the process of a copyright protection. Seemingly, the owners and relatives are currently happy with this pressing problem, which is causing a major hindrance to their right to property. In considering how this issues is to be control, digital fingerprint can be smartly embedded/hidden in to the multimedia contents, in so many ways, by the application of "watermark" processes. Watermarking is a technique used to hide extra information in to the digital content, for the purpose of preventing the illegal copying and redistributions. The watermarking also helps in identifying the original owner of the content. It is conventionally concerns with robustness (ability to withstand supplied change in the embedded watermarks), against the various attack, by the traitors. But this robustness is less effective when tackling the issues of coalition of attackers. The issue of coalition of attackers arises, by considering the average of several copies of the contents together, while extracting new manipulated copy [17]. The goal of watermarking here is; to trace and identify at least one traitor out of the colluders, that participated in such illegality of forming a compromised copy [17,19]. The coalition attack does not hold, if there is only single copy of the watermarked content. [19], but only the pirate users will be identified, while the responsible traitors will be trace free. it is base on this note, to collusion resistant and ability for identification, there by inculcating a deterrence to the collusion attempts by the users. Another signal processing attacks that is not even producing an illegal copy, but the perpetrators publishes their own copies that are indistinguishable (closely same with the original

copy). The scenario can be best understood, that a watermarks are usually called a noise in a SS (speed spectrum) such as DCT. Especially when multiple watermarks copies are presented and certain number of traitors intends to conspire in combines copies, will attain a qualitative content deemed for distribution with general acceptance. The embedded hidden noise of digital watermark in speed-spectrum (SS), has an energetic capability that is deemed in degraded acceptance of a content (Image) quality by the owner (watermark provider). The watermark (noise) may found everywhere within predetermined frequency band [19]. It is specifically noted that by considering the average signal that is differently represented in the copies. It is simply averaging the signal and find their differences, one can obtain a combined signal for a number of watermarked images. The noise is cancelled and original image (less noise) will hold. This is better for defeating an individual (watermark) scheme in a tracing. There are several other schemes that enforces copy right protection, such as "Self enforcement", where the data content is encrypted with the uniquely different decryption key, and very vital information of user are all attached to the content. This will make the user not reveal his key, as he knew that his personal information are attached such as credit card information. It will serve as a simple and effective countermeasure for deterrence of key leakages act by the user.

3.2 Key distribution

In trying to make the information secured to the unintended users, especially in context of subscription channels, where an expected authorised user will be privileged to access a content of data, for example; the propriety channels (pay -tv). The contents of the digital data are protected against the unintended users by using the cryptographic encryption techniques.

A scenario; is when number of channel's subscribers will have to access same content of digitally broadcasted data, and authorised users should be able to use a key given/assigned to each one for the authentication before one can be able to access the content (decryption process). The problem may arises, when the authorised user decided to reveal his decryption key given to him, purposely for him alone, but he share it to other, who are not suppose to access to access it. So, it is important to find a useful mechanism that will counter such leakage of the decryption key.

It is getting worse, if the users have came together to compare their decryption key and identify where it differs, and able to produce another new comprised key, that will serve/act as an authenticator key, and be used by illegal user (pirate users) to access the content. The major concern is to focus on how to securely distribute the assigned key and prevent the broadcasted content to be accessed, by preventing the traitor from redistributing the decryption key, that will an able the pirates to have an illegal access to the content, that has been encrypted for security purposes.

Notably, considered the set of users are assigned a unique private decryption key, differently from the others, so whenever a pirate decoder is found, it is going to be observe that, the pirate decoder uses some of the keys supplied to authorised users. Hopely, it will identify the personal unique key that will link to a traitor, who is involved in the illegal leakage of the key. But when considering the distribution of DVD, it is going to be little problematic, as every copy will have to be different, however in the case of online data is stored encrypted copy individually for each authorised user.

In traitor tracing, there is technical method of identifying that piracy holds, curtailing the transmission of content to unauthorised user, and the process should not harm the innocent users. Lastly a legal evidence for the identity of the pirate traced. Chor et al in their paper "Traitor Tracing" adapted the fact that their scheme (K-Resilient and Simple One Level scheme)"have very desirable property that the identity of the traitor can be established by considering the pirate decryption process as a black box. In order to identify a traitor, it suffice to capture one pirate decoder and examine its behaviour, there is no need to break it or read any data stored inside (pirate decoder means decryption process), this may or may not a physical box and may simply be some code on a computer"[1]. Some of the components in traitor tracing, so called (enabling block and ciphertext block) are important in this techniques, where the enabling block is the phase section that contain all the keys that are encrypted, while the ciphertext block is the actual encryption of the content data[1], with some sort of random key. Usually the mode of tracing in block model, the tracing process sends some devious encrypted message to the pirate decoder, with purpose of determining which key uses, while observing its behaviour. And perform a reverse -engineering on the

pirate decoder which result in trapping a traitor as he perform same operation on a legitimate decoder. This pattern was adapted by Chor et al [1], on (K-resilient scheme and simple one level scheme) respectively. The simple one level; And security assumption of the scheme is of the personal keys base on symmetric encryption. In the general concept of the scheme; the supplier generates a meta keys which is a base set A of random keys and assign subset of these keys to the users, m keys per user (personal), then denotes the personal key for user U by $P(U)$ which is a subset of A ; $(AP(U))$ [1]. The data in a scheme consist of enabling block and cipher block; in which the cipher block is a symmetric encryption of the actual data by the usage of S (secrete random key) or it could be the exclusive-or of the S as such we have $S = S1 \oplus S2 \oplus \dots$. Enabling block consist of the encrypted keys and allows the user to get the secrete key S and compute it by decrypting the value for which has the keys and computes the actual key to get the contents of the data.

By considering the simple one level scheme; where the number of traitors is expected to be one $K=1$ and supplier generate the key in the matrix with $\log n$ rows and two columns; $a_{01} a_{11} a_{02} a_{12} \dots a_{0 \log n} a_{1 \log n}$

Each user has a $\log n$ bit identity and the personal key for user i is the set of $m = \log n$ keys and i th is the bit of user's identity. The key distribution; the data supplier chooses each user has a $\log n$ bit identity and personal key for user i in which the value of and reconstruct a_{li} , both all encryption the S_i 's S_i is encrypted under the two keys of the i th are added to the enabling block while every user and hence can decrypt S . The tracing scheme row U can a_{0i} is used to encrypt the S (is the key in which the cipher text can be decrypted, and S_i is the secrete key to each user) the data is encrypted S from the enabling blocks and then uses the S and decrypt the cipher block, it splits in to $\log n$ secrete of $S_1, S_2, \dots, S_{\log n}$ and is chosen randomly such that S is a bit-wise XOR of the S_i ; $S = S1 \oplus S2 \oplus S3 \oplus \dots S_{\log n}$ and hence the encryption of secrete keys S in the enabling block is; $E_{a_{01}}(S1) E_{a_{02}}(S1) \dots E_{a_{0 \log n}}(S1) E_{a_{11}}(S2) E_{a_{12}}(S2) \dots E_{a_{1 \log n}}(S2) E_{a_{01}}(S_{\log n}) E_{a_{02}}(S_{\log n}) \dots E_{a_{0 \log n}}(S_{\log n})$.

3.3 Pirate Rebroadcast

The digital contents are exposed to the possibility of contents such as (Images, Video, Audio). With no exception, the rebroadcast is also affected with the pirate attack called "pirate rebroadcast attack", usually in this type of attack, it is difficult to trace back the traitor's key in the pirate decoder, as the pirate issued the copy of the digital content as his productions, and be able to revoke the user's key. What normally happens from the source (broadcast publisher) is encrypting the content to be send to the number of users (receivers), it is expected that each user will receive a unique key, which means that the total number of user will have to obtain a key as such the publisher will need to make an effective use of medium, that the content will be transmitted, at the same time to be able to cancel (revoke) any compromised user form in the mist of legitimate (authorised) users.

In the beginning instance for the minor (trivial) solution, private/personal key is obtain by the user, while the publisher will send/communicate to each single user with a length of the ciphertext through a communication medium. Notably, this way causes much squandering of bandwidth, but enhances optimality on a user side. The second solution; the publisher prepares a different keys to assign it to each subgroup of users (receivers), and subsequently each user obtained the key assigned to his subgroups. This enhances the optimality of the ciphertext length an causes the user to unexpectedly store a keys $Xy-1$ ($X=2$, $y=N$), which is so big to be handle by the user.

In the case where the users give out their key, that will allow the unauthorised user (pirate) can have access to the encrypted content, then the pirate can possibly produce a new compromised key that will enable them also to access the content. The user who happened to leak the key is referred as "traitor". This issue can be resolve by employing the traitor tracing scheme [1], where the publisher will engage with the pirate decoder, and carefully observe the responses supplied. The identity of the traitor can be fished out, then immediately revoke (cancel) the identified user (traitor).

3.3.1 Trace and Revoke technique

It is of no use for trace and revoke scheme in respect to pirate rebroadcast attack, as the attacker publishes the key, and the tracing authority will never find any

information regarding the pirated publisher (traitor). The significant measures in curtailing this type of attack (pirate rebroadcast), is to employ the watermarking technique [3]. And each user receives a portion of the content, but this result in the consuming high rate of bandwidth. These types of technique is quite deterministic; that a trace and implicated user will be caught while in some cases, it tends to be probabilistic; where the technique seems to have a minor false in its implications. In this process of trying to apprehend atleast one of the traitor. There are some strategies employed; one is sequential traitor tracing and the other is dynamic traitor tracing [8, 9]. The sequential context; it require to embedded only the mark once in each content for the each receiver (user), while in dynamic scheme, the markings are adaptively embedded in respect to the feedback received from the user's responses. And this (dynamic) is much better in terms of bandwidth utilization, as a portion of segmented content are concurrently propagated in corresponding to the size of bandwidth [8]. For every scheme parameters employed, within the several propagation, the scheme will be able to converge at a certain point to reveal the identity of one of the traitors [5].

From the mentioned techniques in fighting against "rebroadcast attack" by the pirates, it is just tracing and identification, but the most important countermeasure id to remove the pirate user from the list, that are benefiting from unauthorised access [5]. Two encryption are employed, one for the purpose of encrypting the content and the second for broadcasting encryption, but in one way or the other in the course of explain previously, the pirates happened to possess the key, especially in sequential traitor tracing. so far, in the process of revocation. The scheme should be trace and revoke with highest number of unlimited users (traitors) and colluding user in false free suspicions.

3.4 Round Complexity

The round complexity is another form of very significant traitor tracing technique, where a transaction of interaction is engaged between the tracing entity and pirate user (adversary). And observing the amount of communicated- interaction held, in a period of time, for the tracer to be able to identify the identity of the adversary. This technique employs the fingerprint code application for an efficient tracing operation.

The administration of multimedia content to the various numbers of users is sufficiently distributed by meagre enrolling the encryption scheme. Considering this setting In which numerous users are expected to portion the same decryption capability, it is logical to expect some bad (Adversary) could have get some legitimate user keys and disseminate to others. In any way of stopping this illegal act of emanating the users secrete key, the curtailing operation can be constructed in to the encryption scheme. This type of context where the number of users are more, the efficient capability of tracing entity to interact with the generated pirate decoder and able to identify at least one of the users identity who take part in the illegal act of releasing his key to the unauthorised pirate decoder, this ultimately leads to the scheme best known as traitor tracing.

The detail description of traitor tracing scheme and constructions was previously elaborated by Chor, Fiat, and Noar [1] the preference parameters imprecise in this setting are;

- The size of storage required in the users entity
- The length of the cipertext minimization
- The length of the encryption's key the fingerprinting code is adaptively strategies in respect to the traitor tracing scheme, depending with quite number of transactions stipulated to the codeword generation in a number of proportional distributions. In a previous conventional settings of traitor tracing schemes, the original code- word is defined with specific static setup phase length at the very beginning for codeword generation and embedded in to the content of the whole data with property steps involve in the tracing in fingerprinting which includes; It is considered to be a unique ID to the each corresponding user which produces an output as a set of string of a certain length that may be a function to other parameter which (either be deterministic or probabilistic) and will name fingerprinting code according to the properties underlying procedure. The codeword will be kept secrete in order to prove for the benefit of identify a traitor, but as coalition has less information in constructing the pirate code- word, in which in many cases the actual deployment of fingerprinting code, the public code will be preferred. Forging Algorithm; is the in the context of fingerprinting code, the set of code- words that can be produced by a pirate using the codeword owned by authorised user. So in the process

the forging would be corresponding to producing a valid pirate codeword out of original codeword available to the traitor and will be enforced by marking assumptions. When users collude, they can find the difference of the marks in between their object codeword, but the aimed property of the marks is that the user of the object cannot make any alteration on the object content, if they cannot find the marks in the object in which subsequently makes it useless and these property leads to what is known to be a "Marking Assumption". After the codeword are randomly generated, and the forging algorithm have taken by the pirate user to produce the valid codeword, the tracer will run identification algorithm hoping to identify a codeword that was given to one activities of piracy (piracy) who took part/role in the illegal activities of piracy/forgery. This algorithm runs over many subset obtained in a fully-collusion restricted code. This is what is happening in the traditional way of traitor tracing/tracking, but in this new scheme is provided which is expected to sufficiently work effectively by making the fingerprinting code shorter and robust in tracing the traitor and will not allow a whole detrimental to be made by the pirate user before they should be traced and identified.

Adaptive formation of fingerprinting is a dynamic phenomenon for the assignment of codeword generation and tracing schemes. The concept is codeword is generated in a partitions proportion embedded with the content of the data to be distributed to users, and the authority is observing the behaviours of the first released partitioned content object data and when they (authority) find copy of the illegal duplicate content data other than the one legitimately assigned to, then the responsibility of the tracer is to generate the identification algorithm for tracing. Notably the number of users N is divided in to subset with respect to the size and implementation through "Walking Procedure". The user set will be updated to the new current partition and generate and assigned the new codeword in the fingerprinting code, from the walking argument that is usually involve to every conventional tracing scheme, to this also was involves by taking the pattern of the ciphertext in a random fashion until coming to a certain point where the pirate decoder could not decrypt the ciphertext. This process is repeatedly continuous with various different portions of the subsets. After all the observations of the of the subset behaviour of the resulting output will infer a corrupted user identity.

CONCLUSIONS

In the contained elements of fingerprinting form all mentioned above areas, information is invisible to the information and these hidden information should be robust against any form of attacks and when collusion of various user to yield a new form of product (remember the traitor tracing scenario). And ultimate result will be possible to find atleast one of the users in the collusion team. We will noticed that some of these techniques; Watermarking, Fingerprinting, stenography are all stipulated on just inserting the hidden information, mainly for intended purposes. Because there are number of issues specifically covered with production and communication of digital contents, through a media. The watermark embedded the information that identify the ownership/copyright details in the content (object), while fingerprinting code hide identification, it recognizes the user. These terms are going to be used interchangeably (fingerprint and watermarking). The motive behind improved fingerprint code sacrifices to any modification to the object (content) that may jeopardise the fingerprint shall result to the object useless. And the robust

nature of fingerprint code technique needs its attachment to the object (content) to be perceptually significant [3].

REFERENCES

1. Benny Chor, Amos Fiat, Moni Naor, and Benny Pinkas. Tracing traitors. *IEEE Transactions on Information Theory*, 46 (3):893–910, 2000.
2. Aggelos Kiayias and Serdar Pehlivanoglu. Tracing and revoking pirate rebroadcasts. In *International Conference on Applied Cryptography and Network Security*, pages 253–271. Springer, 2009.
3. Aggelos Kiayias and Serdar Pehlivanoglu. Improving the round complexity of traitor tracing schemes. In *International Conference on Applied Cryptography and Network Security*, pages 273–290. Springer, 2010.
4. Hans Georg Schaathun. The boneh-shaw fingerprinting scheme is better than we thought. *IEEE Transactions on Information Forensics and Security*, 1 (2):248–255, 2006.
5. Fabien Petitcolas. Anderson. rj, “evaluation of copyright marking systems”. In *Proceedings of the IEEE International conference ‘in Multimedia Computing and Systems (ICMCS’99)*. Florence, Italy, volume 1, pages 574–579, 1999.
6. J Mark Ettinger. Steganalysis and game equilibria. In *International Workshop on Information Hiding*, pages 319–328. Springer, 1998.
7. Jeffrey L Duffany and Marcus D Velez. Steganography and steganalysis in digital images. Technical report, DTIC Document, 2012.
8. Christian Cachin. An information-theoretic model for steganography. In *International Workshop on Information Hiding*, pages 306–318. Springer, 1998.
9. Nicholas J Hopper, John Langford, and Luis Von Ahn. Provably secure steganography.
10. In *Annual International Cryptology Conference*, pages 77–92. Springer, 2002. 2710. Jun-Jie Lai. Image watermarking techniques.
11. Alphons AML Bruekers, Geert FG Depovere, Petrus ACM Nuijten, and Arnoldus WJ Oomen. Embedding supplemental data in an encoded signal, such as audio/video watermarks, December 5 2000. US Patent 6,157,330.
12. Minoru Kuribayashi and Hatsukazu Tanaka. Fingerprinting protocol for images based on additive homomorphic property. *IEEE Transactions on Image Processing*, 14 (12):2129–2139, 2005.
13. Ingemar J Cox, Matthew L Miller, Jeffrey Adam Bloom, and Chris Honsinger. *Digital watermarking*, volume 1558607145. Springer, 2002.
14. Stefan Katzenbeisser and Fabien Petitcolas. *Information hiding techniques for steganography and digital watermarking*. Artech house, 2000.
15. Dan Boneh and James Shaw. Collusion-secure fingerprinting for digital data. In *Annual International Cryptology Conference*, pages 452–465. Springer, 1995.
16. Kaoru Kurosawa and Takuya Yoshida. Linear code implies public-key traitor tracing. In *International Workshop on Public Key Cryptography*, pages 172–187. Springer, 2002.
17. Emil Praun, Hughes Hoppe, and Adam Finkelstein. Robust mesh watermarking. In *Proceedings of the 26th annual conference on Computer graphics and interactive techniques*, pages 49–56. ACM Press/Addison-Wesley Publishing Co., 1999.
18. Cecilia Deleralee. Identity-based broadcast encryption with constant size ciphertexts and private keys. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 200–215. Springer, 2007.
19. Yi Ding and Lei Fan. Traitor tracing and revocation mechanisms with privacy-preserving. In *Computational Intelligence and Security (CIS), 2011 Seventh International Conference on*, pages 842–846. IEEE, 2011. 28
20. Yacov Yacobi. Improved boneh-shaw content fingerprinting. In *Cryptographers’ Track at the RSA Conference*, pages 378–391. Springer, 2001

HOW TO CITE: Ibrahim Nasir Aliyu, Unified Model for Fingerprinting Code Applications, *Int. J. Sci. R. Tech.*, 2026, 3 (10), 851-860. <https://doi.org/10.5281/zenodo.23340806>