ENCRYPTED | PROTECTED

Six Degrees Counterfeit Prevention, LLC.
5737 Kanan Rd. #462
Agoura Hills, Ca. 91301

818-570-1277

www.6dcp.com

WHITE PAPER

CRYPTOCODEX LTD. TECHNOLOGY

CONFIDENTIAL

ABOUT US

Cryptocodex Ltd., developed the most advanced and secure counterfeit protection, track & trace, and document security solutions in the world.

In 1999, Cryptocodex Ltd, an Israeli company with a background in cyber security and cryptography, envisioned a future where words like zero-day attacks, brute force, cryptanalysis and malware will become common knowledge. A time when vulnerabilities in operating system, software application, and infrastructure that contain sensitive information such as credit card details, ID, driver's license, passport and visa information, property, automobile or health insurance cards, etc. will become a target for cybercriminals worldwide.

Regardless of their motives, cybercriminals understand the simple principle that; if it is connected to the Internet, it can and will be hacked…if it hasn't been already. Governments, financial institutions, corporations etc. are aware of this threat, and are left with no alternatives but to invest in stronger networks, tougher encryption, and other technologies to protect themselves. Unfortunately, those highly secure systems are built with the same vulnerable components, and are constantly exposed.

And despite all the resources poured into security, the threat is not only imminent, it is rising exponentially - as evident in the countless articles on breaches to the FBI, CIA, Google, Microsoft, Oracle IMF, Citibank, etc. database infrastructure(s). The result of which can lead to financial losses, counterfeit products, credit and identity fraud and sometimes, loss of human lives.

Albert Einstein once defined insanity as doing the same thing over and over again and expecting different results.

So now the question remains. If there is a solution to the problem, what does it look like? Where would you store critical data if not on a centralized database? How would you secure the content? And how would law enforcement officials, customs agents, corporate investigators and consumers verify the authenticity of the product/document?

Noticing the dire demand for real and effective, multi-platform solutions, Cryptocodex Ltd utilized a breakthrough in cryptography to develop a process referred to Micro Database Less Encapsulation, or MDLE. With MDLE, critical information i.e. Driver's license (name, address, age, DL#, and issuer) is encrypted and encapsulated into an affordable data carrier such as a 2D barcode or RFID/NFC tag. Affixed or printed onto the document, the data carrier securely contains all of the holder's information plus the data required to authenticate the document and it's content. Access to authentic information is accessed via any barcode reader, cell phone camera or RFID reader. Following in the philosophy of financial investors – to never place all your eggs in one basket, MDLE eliminates the need to maintain critical information on [vulnerable] online database. And by eliminating a target for cybercriminals, you reduce the threat.

Link to Patent

ABSTRACT

A method for rearranging a data segment. The method comprises providing a data segment containing digital content, generating a set of human dependent variables according to a plurality of human related activities, rearranging the data segment according to the set of human dependent variables, and updating a log according to the rearranging. The digital content may be retrieved from the rearranged data segment according to the log.

DESCRIPTION

FIELD AND BACKGROUND OF THE INVENTION

The present invention, in some embodiments thereof, relates to a method and a system for verifying the data authenticity and, more particularly, but not exclusively, to a method and a system for verifying the authenticity of data transfer, process, and storage.

SUMMARY OF THE INVENTION

According to an aspect of some embodiments of the present invention there is provided a method for rearranging a data segment. The method comprises providing a data segment containing digital content, generating a set of human dependent variables according to a plurality of human related activities, rearranging the data segment according to the set of human dependent variables, and updating a log according to the rearranging. The digital content is retrieved from the rearranged data segment according to the log.

Optionally, the method further comprises adding unrelated content to the data segment before the rearranging.

Optionally, generating is performed by a computing unit, the generating comprising recording the plurality of human related activates from a routine operation of the computing unit by a human user.

More optionally, the routine operation is an input recorded from a group consisting of manipulating of a mouse pointer and typing a sequence of letters.

More optionally, the recording comprises recording an audio print of the voice of the user, the human characteristics comprises features extracted from the audio print.

More optionally, the recording comprises recording a fingerprint of the voice of the user, the human characteristics comprises features extracted from the fingerprint.

More optionally, the recording comprises analyzing information related to a profile of the user, the human characteristics comprises features extracted from the analysis.

More optionally, the generating is performed by a computing unit, the recording comprises capturing at least one biometric characteristic related to a user operating the computing unit.

More optionally, the at least one biometric characteristic comprises features extracted from an image of the user.

Optionally, the method further comprises compressing the data segment before the rearranging.

Optionally, rearranging comprises dividing the data segment to a plurality of arrays and rearranging the plurality of arrays according to the human dependent variables.

More optionally, the plurality of arrays comprises at least one of a subgroup of arrays each having a different size and a subgroup of arrays each having a different number of dimensions.

More optionally, the dividing is performed according to the human dependent variables.

More optionally, digital content stored in at least one of the plurality of arrays is rearranged according to the human dependent variables.

More optionally, the rearranging comprises further rearranging the divided rearranged data segment according to the human dependent variables.

More optionally, the rearranging comprises dividing the set of human dependent variables to a plurality of subsets and using each the subset for rearranging at least one of the plurality of arrays.

Optionally, the method is executed using a computing unit, the rearranging comprising halting a plurality of processes executed on the computing unit during the rearranging.

Optionally, the method further comprises dividing the data segment to a plurality of data sub-segments and spreading the plurality of data sub-segments among a plurality of computing units; wherein the digital content is retrieved after the plurality of data sub-segments are gathered.

Optionally, the method further comprises dividing the log to a plurality of subsets and spreading the plurality of subsets among a plurality of computing units; wherein the digital content is retrieved after the plurality of subsets is gathered to reconstruct the log.

Optionally, the digital content comprises identification information related to an article, further comprising using the rearranged data log for tagging for the article.

More optionally, the tagging allows the authentication of the article.

Optionally, the data segment is hosted in a memory device, the method being performed in response to a deletion of information stored in the data segment.

According to an aspect of some embodiments of the present invention there is provided a method for forwarding a data segment. The method comprises providing a data segment containing digital content at a source computing unit, generating a set of human dependent variables according to a plurality of human related activities, rearranging the data segment according to the set of human dependent variables, logging the rearranging in a rearranging log, and forwarding the rearranged data segment and the rearranging log to a target computing unit.

Optionally, the target computing unit may retrieve the digital content from the rearranged data segment by using the set of human dependent variables according to the rearranging log.

Optionally, the method further comprises verifying the target computing unit before the forwarding.

More optionally, the verifying is based on at least one of the internet protocol (IP) address, the media access control (MAC), and the hardware identification of the target computing unit.

Optionally, the forwarding comprises halting a communication of at least one of the source and target computing unit.

Optionally, the forwarding comprises separately forwarding the rearranged data segment to the rearranging log target computing unit.

Optionally, the forwarding is performed over a peer-to-peer (P2P) connection.

Optionally, the generating further comprises generating a first segment of the human dependent variables in the source computing unit, generating a second segment of the human dependent variables in the target computing unit, and combining the first and second segments for generating the set of human dependent variables.

Optionally, the method further comprises forwarding the first segment to the target computing unit, allowing the target computing unit to use the first segment for rearranging the second segment and forwarding the rearranged second segment to the source network, and allowing the source computing unit to use the first segment for retrieving the second segment from the rearranged second segment. The combining is separately performed in each the computing unit.

According to an aspect of some embodiments of the present invention there is provided a system for rearranging a data segment. The system comprises an input module configured for receiving a data segment containing digital content, a capturing module configured for recording a plurality of human related activities and generating a set of human dependent variables accordingly, a rearranging module configured for rearranging the data segment according to the set of human dependent variables, and a logging module configured for logging the rearranging. The logging allows the retrieving of the digital content from the rearranged data segment.

According to an aspect of some embodiments of the present invention there is provided a method for generating a unique identification tag to an article. The method comprises providing an identification segment containing identification information, generating a set of random variables according to a plurality of human related activities, rearranging the identification segment according to the set of random variables, and tagging an article with the rearranged identification segment. The identification segment is retrieved using a log of the rearranging.

Optionally, the random variables are human dependent variables generated according to a plurality of human related activities.

Optionally, the tagging comprises associating the article with a tag comprising the rearranged identification segment, the tag being selected from a group consisting of: a barcode, a radio

frequency identification (RFID) tag, a machine-readable visual representation, and a machine-readable audio representation.

Optionally, the method further comprises allowing an authentication of the article by the retrieved identification segment.

Unless otherwise defined, all technical and/or scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which the invention pertains. Although methods and materials similar or equivalent to those described herein can be used in the practice or testing of embodiments of the invention, exemplary methods and/or materials are described below. In case of conflict, the patent specification, including definitions, will control. In addition, the materials, methods, and examples are illustrative only and are not intended to be necessarily limiting.

Implementation of the method and/or system of embodiments of the invention can involve performing or completing selected tasks manually, automatically, or a combination thereof. Moreover, according to actual instrumentation and equipment of embodiments of the method and/or system of the invention, several selected tasks could be implemented by hardware, by software or by firmware or by a combination thereof using an operating system.

For example, hardware for performing selected tasks according to embodiments of the invention could be implemented as a chip or a circuit. As software, selected tasks according to embodiments of the invention could be implemented as a plurality of software instructions being executed by a computer using any suitable operating system. In an exemplary embodiment of the invention, one or more tasks according to exemplary embodiments of method and/or system as described herein are performed by a data processor, such as a computing platform for executing a plurality of instructions. Optionally, the data processor includes a volatile memory for storing instructions and/or data and/or a non-volatile storage, for example, a magnetic hard-disk and/or removable media, for storing instructions and/or data. Optionally, a network connection is provided as well. A display and/or a user input device such as a keyboard or mouse are optionally provided as well.

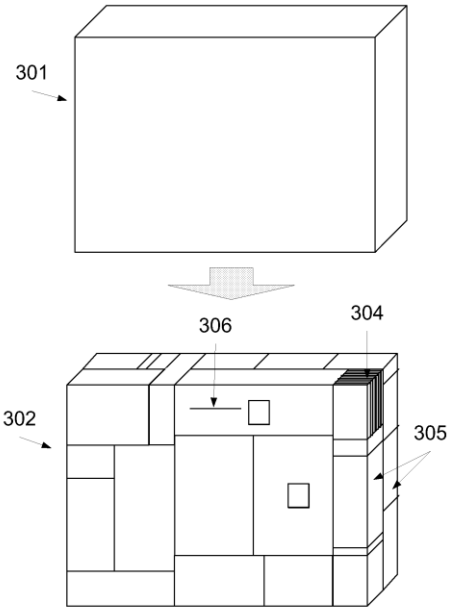

FIG. 5

301 - Data Input

302 - Randomly split data into non-symmetrical (binary) blocks

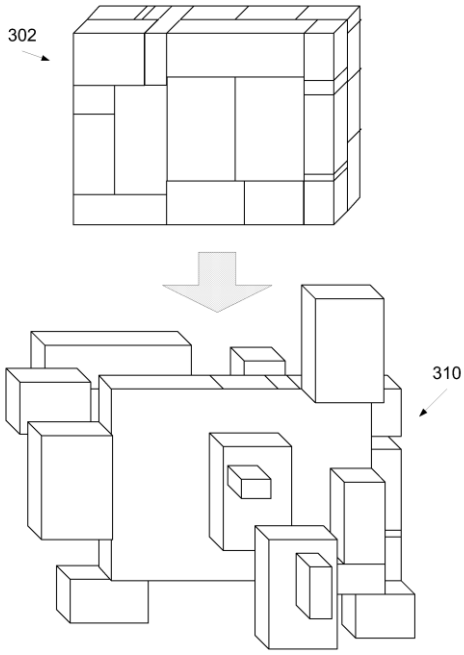

FIG. 6

310 - Data is (true) randomly shuffled and salted with a unique salt per block according to the Pure Human Randomness (PHR) function

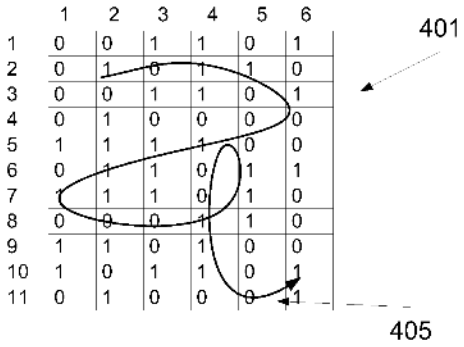

FIG. 7

After data blocks have been salted and shuffled, each sub block is re-shuffled with white noise

THE ENCRYPTION METHOD (SIMPLIFIED):
Step 1: A state of the art compression algorithm optimizes the original content for efficient performance of the encryption engine.

Step 2: Salting the original content with white noise and PHR (Pure Human Randomness).

Step 3: Using a unique modifier, the encryption engine creates both a shuffle and move command that is based on the PHR and white noise engines, and performs the first layer of modification to the original content.

Step 4: XOR function on the PHR output results in a Random Oriented Enhanced Encryption (ROEE). When combined with a time set of instructions and a computational temporary set of instructions, the result is a real one time pad (OTP). This appears as a polymorphic function where the output (encrypted content) is variable.

Step 5: Reconstructing a file level on a multiple N-dimension code manipulation with zero use of a calculative algorithm, also referred to as a secondary phase of salting, results in superior protection against Rainbow Crack, Dictionary Attack, Cryptanalysis, etc.

PERFORMANCE FEATURES: Key
Strength – 1 million bit or more
Performance 400% faster compared to AES.
MPU use – Mathematical Process Unit in CPU use 3% –
7% only. Overhead of the file from original 5% +/-
(original+5%) +/-

Other encryption algorithms have a bit overhead of between 300-700% when encrypting small amounts of information. PHR on the other hand uses an unparalleled, non-dictionary, compression ratio operational technique that produces a bit overhead of 5-7%. Because of this, PHR is capable of encrypting entire columns of a database (up to 500 characters) into one 2D barcode. A process referred to as MDLE – Micro Database Less Encapsulation.

QUOTES:

"I worked with this group and was in charge of their technical development team in Haifa.

The algorithms were extremely fast for encryption/decryption with a reasonably low overhead of added bits to the content. Commercial viability and adoption were a key stumbling block for market introduction. However, as a cryptographer, I performed sufficient statistical analysis to indicate that it was good enough to prevent both a brute force attack or mathematical pattern analysis.

The use model was specifically designed to prevent man in the middle attacks and that is why the session key could change at different levels of granularity - all the way down to the packet level (*bit of overkill*). Shifting session keys prevent the middle man from creating the next key since you had to have access to the first key used. This approach has some serious deficiencies but was an excellent replacement for standard SSL methods.

2d-Barcodes - While I did not work with Privacy Inside (now Cryptocodex) on this application, I did a preliminary analysis of their merging barcodes with PHR and found this approach a strong audit tool for counterfeit commercial goods (electronics, apparel, accessories). With the new smartphones, you could use an online camera to capture the image and interrogate a server using cellular data services. This method is already implemented for 2D barcodes on coupons that can be scanned at a point of sale laser scanner.

Their application is easy and practical to implement, unlike other methods that create embedded codes in the material or paints used.

The encrypted barcode is an *excellent* add on to document protection, especially those produced by Word and Adobe. I wish them well.

Most of the scientific work was developed by Royi Cohen, a smart young man whom I enjoyed for his sincerity, inventiveness and honesty."

- Andre Szykier

"I believe that Cryptocodex/QMarkets* have a very promising technology at hand for the payments industry and coupled with the extremely interesting idea of creating a new currency to work together with this technology they may have a winning proposition with great potential."

- Avivah Litan

Cryptocodex – Provider of QRedit: Credit Card Cyber Defense System
QMarkets – Crytpo Currency