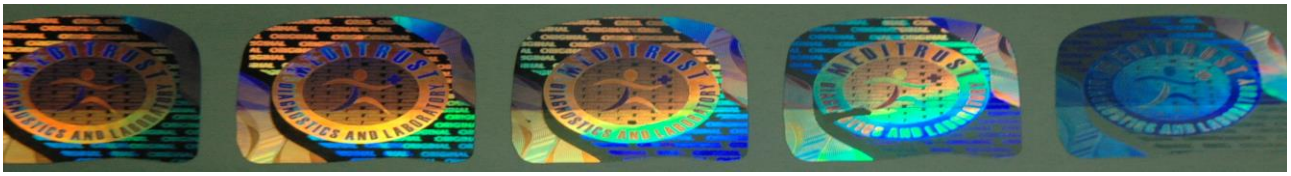


Why Security Holograms? - A White Paper

Dr.P.T. Ajith Kumar, President and Leading Scientist,

Light Logics Holography and Optics, Trivandrum, INDIA – 695027. www.lightlogics.in

The author is the President of Asian Anti-counterfeit Association (AAA) - India Chapter and the Convener of the Working Group on Optical Security, Optical Society of India. He was the Team Leader of the Team that set up the first governmental holographic tax stamp Production House of India, that has so far produced over 10 billion tax stamps. He was the Deputy Director of the Optical Image Processing Division, Centre for Development of Imaging Technology (C-DIT), Government of Kerala. Recently he has been selected as Distinguished Fellow – New and Emerging Areas, by the Government of India. He is the recipient of two consecutive Innovation Gold Medals instituted by the Lockheed Martin – USA, Indo-US S&T Forum, University of Texas at Austin, Department of Science and Technology – Government of India and the FICCI. He was a Senior Research Fellow of the Council of Scientific and Industrial Research and had his Ph.D in laser holography from the Cochin University of Science and Technology. He has over 30 years' hands on experience in laser holography.

1. Counterfeiting, a global menace

Creators of original products spend huge money and effort to build a market for their products, by addressing years of customer satisfaction and there by building its goodwill and a brand. Apart from huge funds, advanced product research and market research, proper positioning of the product in the market is highly essential for effective brand building. This is applicable right from ordinary consumable products to high value lifesaving medicines. On the other side, counterfeiters see this as an opportunity to make quick and easy money. They flood the market with substandard duplicate products with identical packaging and labeling. Counterfeiting can not only affect the sales of original products, but leads to destruction of its brand image due to sales of substandard products in disguise. Customers are cheated and reduced customer satisfaction and poor sales can in turn lead to closure and death of a once successful industry.

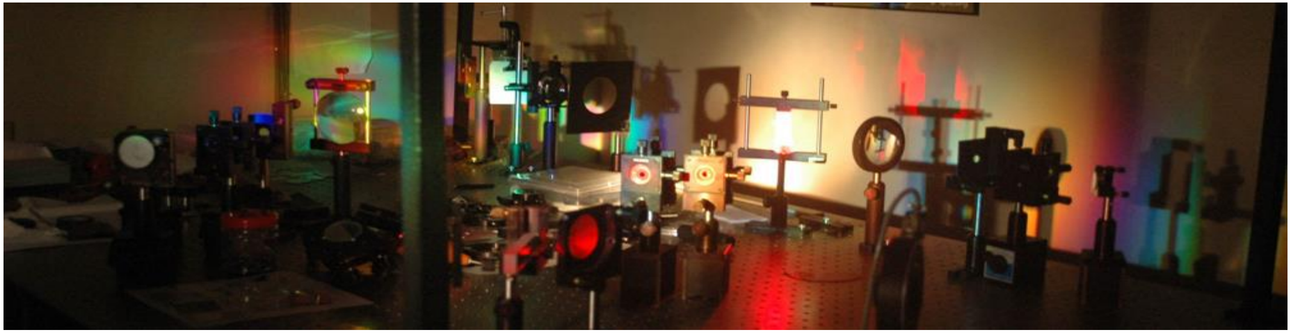
Counterfeit production and distribution take place even in fundamentally important sectors such as food, medicines and core documents. Unfortunately most of the governments fail in effectively addressing the issue. This leads to many sociopolitical issues, huge revenue loss and can even severely affect the progress of a nation. Counterfeiting has globally grown as an illegal parallel industry and they, in reality, wage a tacit war against governments, original manufacturers and law abiding citizens of all nations. Several international studies have proven that a major part of the huge profit from counterfeit production, including counterfeit currency, is pumped into terror and insurgent activities. This gives a big twist to the whole scenario and strongly stresses the need for international initiatives and joint actions to effectively prevent counterfeiting.

2. Counterfeiting, Digital Imaging and Image Processing

The advent of digital computers and accessories such as high resolution scanners, copiers, cameras, and color printers with super realistic image output have made copying and replication of printed documents and product packaging easy. This, along with the applicability of standard image processing software tools, has resulted in very easy and widespread counterfeiting and forgery of original products and documents. Thus the good old 'sanctity of photographic evidence' is lost and it has reached a stage that even moving images are manipulated and documents and ID Cards with advanced printed security features are counterfeited. Recent decades witnessed intense developments in many branches of science and technology Currently we live in a world where sophisticated DNA structures, the basic building blocks of life, can be replicated so as to clone and recreate identical living structures. An Atomic Force Microscope (AFM) that has advanced digital tools can image with ease even to the level of molecules. Since counterfeiters gain huge profit and function as parallel financial forces, they have access to latest technologies and can easily apply state of the art tools to further flourish their illegal business and criminal intensions.

3. Holography

Optical holography is the technology to record and recreate light fields with its whole information content. Holograms are light diffracting structures that selectively scatter and modify light rays falling on them. This way, a peacock feather is a natural hologram. Interference of laser beams is generally used to create holograms and holograms record and recreate light fields emanating from an object or a scene in its most faithful manner. The reconstructed light field from the hologram fills space. Since the light field is reconstructed in its truest manner, it preserves the dimensionality and parallax of the subject and the viewer whose eyes collect the light gets the visual feel that the subject is truly present there. The observer gets attracted to the stunning 3D features of the image and this caused the general belief that holography is just another 3D imaging technology. But holography is much more than this and a technology of immense applications in several avenues of science and technology. Based on the recording methods, holograms can create monochrome or color images. The micro structure of holograms can be a variation of light transmittance, thickness or refractive index. In the eighties holograms emerged as a highly effective and attractive security device and presently this is one of the most popular applications of holography.



A Holography laboratory (*Courtesy – Light Logics Holography and Optics*)

4. Security Holography

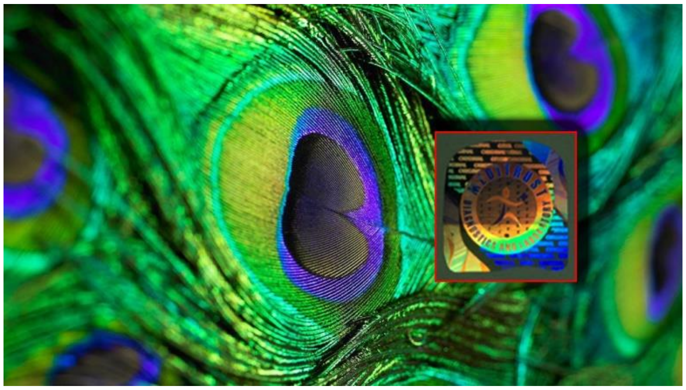
Common security holograms store images and information as complex light scattering microscopic thickness structures. Master hologram origination and conversion of the master relief structure into hologram are two basic and integral processes involved in security hologram production. Master origination involves various intricate steps that need fusion of several technologies and skills. Initially a primary hologram, based on the artwork given by the client, is recorded in special grade photoresist material coated on high quality glass. This primary master is popularly known as the Glass Master. Classical light interference or optical projection of computer generated structures (fringes) can be applied to create complex diffracting structures in Glass Master Holograms. Based on the technology applied, security holograms are broadly classified as Classical 2D/3D, Classical 3D, Dot-matrix and Electron Beam holograms. In Classical 2D/3D holography, 2D layers of images are superposed to form a 3D holographic image structure that has different image layers arranged one over the other, as foreground, middle ground and background. In Classical 3D security hologram mastering a true 3D artwork or a statue with intricate image content is used to record a glass master hologram. In Dot-matrix mastering an array of dots or computer generated image fields are recorded in the photoresist emulsion by applying specialized mastering machines with lasers, quality optics, precision opto-mechanics and advanced security software that simulates the diffractive structures, as per the hologram design. In Electron Beam Hologram mastering, a fine beam of electrons are used to record complex computer generated holographic structures in special type of photoresist materials. It is possible to create 2D/3D and 3D holographic image content by using Dot-matrix and E-Beam hologram mastering too. Each mastering method above has its own merits and demerits and to achieve extreme high security, a combination of the above technologies is applied in advanced applications such as passports, national IDs, VISA and banknotes.

The Glass Master Hologram is then coated with a conducting layer of silver and a metal Stamping Shim is prepared through electroforming. The conducting layer formation can be done either through spray metallization or vacuum coating. This Stamping Shim is applied to stamp an array of holograms on a fine grade polycarbonate sheet, which is a thermoplastic material, by applying heat and pressure. This hologram array formation process is known as Image Recombination and various size formats (narrow and wide-web) ranging from 150mm to 1500mm are popular in the industry. Alternative technologies such as UV recombination, optical recombination etc., are also applied to gang up the image. The recombined polycarbonate master is coated with a silver layer and a master hologram is produced again through electroforming. This master is popularly known as Grandmother Master, which in turn is used to produce a set of Mother Masters. From the Mother Masters several Daughter Shims are formed and these Daughter Shims are used to emboss and produce the holographic structures on metallized polyester films, by applying heat and pressure. Hence traditional security holograms are popularly known as embossed holograms. Conversion of the master hologram into commercial grade security holographic stickers involve many other steps such as adhesive coating, die-cutting/ slitting, image transfer etc. From a family of Mother Masters formed from a single Grandmother Master, it is possible to produce many billions of security holograms.

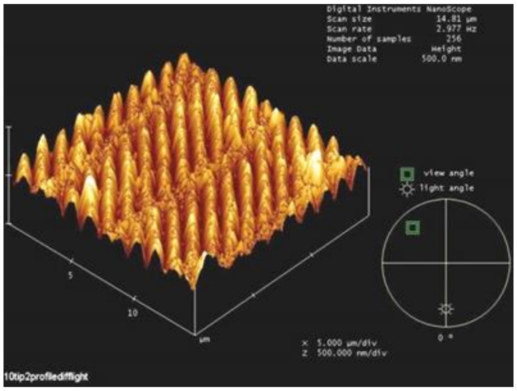
5. Why Security Holography?

The holographic diffracting structure of traditional security holograms is a complex microscopic thickness variation. Such relief structures have interesting light scattering and information storage abilities of immense importance in product / personnel authentication and document security.

There are various facts that add security value for embossed holograms. Just as it is impossible to photocopy a peacock feather, it is impossible to duplicate a security hologram by applying conventional digital imaging tools.



A peacock feather and a security hologram

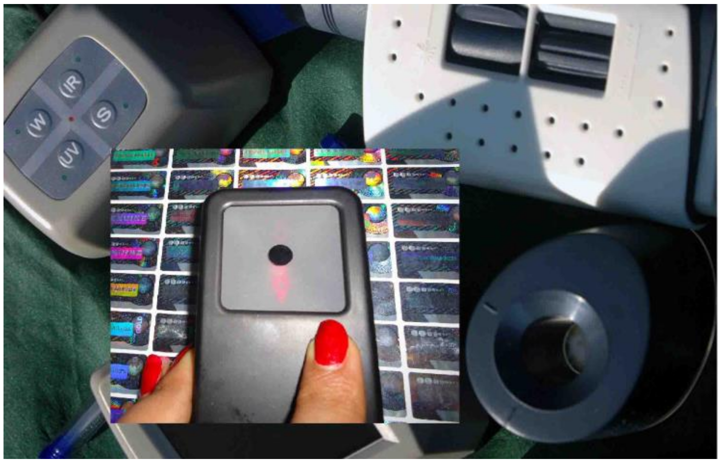


AFM image of a security hologram

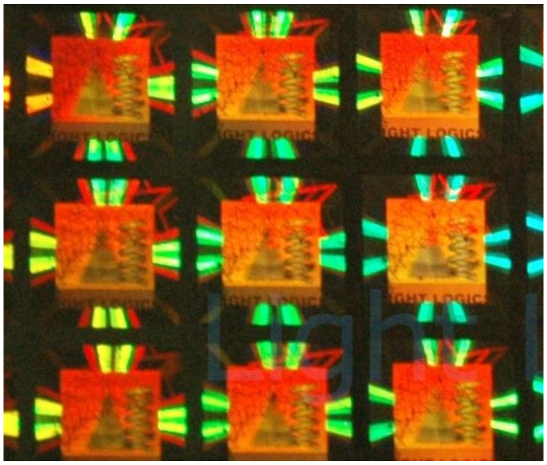
Even for the originator, it is virtually impossible to duplicate a well-designed hologram, with 100% exactitude. A hologram produces images through diffraction and can hold immense amount of data. By scanning the eyes from left to right and top to bottom of a hologram, it is easy to understand the optical variability of a security hologram, in terms of color and image content. A set of overt and covert image content such as specific colors, image movement, micro features, laser readable images, coded features etc. can be incorporated in a security hologram. The micro structure and features of security holograms are so tiny that it opens up scope for advanced forensic level verification and legal sanctity for the authentication process. Above all, security holograms are not very costly and can be mass replicated from the master. This makes it a reliable high end and cost effective security device. Due to these reasons security holograms are widely applied on bank notes, original products, credit cards, identity cards, certificates and documents of high value.

6. How to verify a security hologram?

There are several cases where printed packaging of counterfeit products are so identical to the original that even the original brand owner will not be in a position to correctly authenticate the product. It is the diffractive nature of the security holograms and their complex microscopic structural content that give security value for a hologram that is affixed on the product pack or the document that help the original manufacturer or enforcement to authenticate a hologram. There are various levels for the authentication of a security hologram. These are Primary Verification, Advanced Verification and Forensic Level Expert Verification. Primary Verification is done by inspecting a set of overt features of the hologram under a specific lighting condition. Effective Primary Verification needs a reference hologram and it is done by comparing the overt features of the reference hologram with that of the hologram under test. If the hologram under test is a counterfeit, generally it is possible even with naked eye to detect variations in the image content and the color distribution. If variations are evident, the hologram will be put to further testing. Advanced security hologram verification applies gadgets such as magnifiers, Covert Laser Readers (CLR), Image Decoders etc. A set of knowledge based features are used to do the Advanced Verification. Forensic level authentication involves verification of a set of complex micro features by applying high resolution imaging devices.



Various accessories for authentication



A master hologram

A basic question that frequently arises in security holography is that 'who will do the primary authentication?' Always it is ideal to have the primary verification done by the end users. However, with security holography the situation is a little tricky. During the initial days of emergence of security holograms, several brand owners and governments advertised image features to be looked for in a specific hologram. This lead to the production of inferior 'look alike' holograms with those specific features only and resulted in situations where customers procured counterfeit goods with added confidence inducted by the hologram, by thinking it as original. However fusion of holography with modern information communication technologies has helped a lot to effectively address the above situation and now customers can easily and effectively apply this to do primary authentication of a product.

7. Legal Sanctity of Security Holograms

ICT based machine readable codes are effective in doing customer level primary verification. Since such basic codes can be easily duplicated, there is no legal sanctity for these codes. For example a photocopy of a barcode will also be read by the barcode reader. If the billing is linked to the product database of the original manufacturer, it can detect the fake product provided the original with the same barcode is already billed elsewhere. If it is the counterfeit that is billed first, the system will earnestly bill it as an original product and under legal scrutiny such cases will fail in the court. If a duplication of the barcode is detected by the system, then the product will have to be taken for several advanced level physical and chemical testing. With regard to counterfeit documents the situation is more tricky and involved. If a security hologram is effectively integrated to the product or the document, it is easy to effectively authenticate the product.

Embossed holograms are widely accepted as high-end security devices with many levels of security content. Security holograms can be authenticated through a set of means and forensic level verification can also be done. This gives added legal sanctity for security holograms, compared to ordinary printed features, as per standard forensic practices and laws. However, in a specific legal system, to ensure legal sanctity for holograms, it is essential to have proper law making. Registration of the security hologram, designing the hologram with registered trademarks, specific photographs etc. are important in achieving added legal value for a security hologram.

8. Security Printing and Holography

Generally, quality printing involves creation patterns through color or monochrome ink dots of about 200 to 300 dots per inch (dpi). A 600 dpi color scanner and a quality color printer can be used to easily duplicate such printed image content. Under proper illumination, ultraviolet and infrared hidden images can be scanned into a computer and effectively duplicated. High end printed security features such as tactile printing, printing by specific laser florescent inks etc. are difficult to copy and reengineer to produce duplicate copies. Though not very easy, there are various methods to replicate or duplicate printed tactile contents too. Thus, most of the features in traditional security printing can be duplicated directly or indirectly, with great exactitude, by applying digital tools and printing machines. On the other side classical 2D/3D security holograms can contain complex micro structures of about 3000 fringes per mm. High quality Dot-matrix master holograms can contain over 5000 dots per inch that hold over 25000 lines per inch (lpi). Hence compared to printed security features, it is very difficult to duplicate a well-designed hologram, with full exactitude. Microstructures with resolution above the diffraction limit will not create visible holographic effect and it is important to note here that resolution of the hologram alone will not decide its security.

9. Counterfeiting Security Holograms

It is a basic assumption in security imaging that ‘anything manmade can be counterfeited’. In a way this is true with security holograms too. We have already discussed that scientific developments in the recent decades have made it possible to replicate even complex DNA structures and we are living in such an era. This way, security holograms are also attacked by counterfeiters. They try to do reverse engineering and re-mastering or do copying from the original embossed hologram and then do a re-mastering. Reuse of holograms is another threat being faced by the original manufacturers and governments. Since holograms are produced in volume and affixed on mass moving products and documents, it is not practical to individually authenticate the product through manual Primary Verification of the hologram.

10. Machine Readable Codes and Security Holography

Barcodes are machine readable codes that facilitate automation. Barcodes help supermarkets to do quick billing and the supply chain network to have easy access to specific database and track a particular product. If the identity card or health card of a person carries a barcode, it can help to immediately switch the data of a person, from a database. There are several types and formats of barcodes. Traditional barcodes are printed as a set of black lines with white space in between. 2D barcodes and data matrix arrays can hold more data and can be read with traditional imaging devices. QR Code is a typical example of a popular, easy to generate and read 2D barcode. However, barcodes can be easily photocopied and the copy will work as effectively as the original.

Thus, it is easy to duplicate and reuse barcodes. Barcodes can be further encrypted to ensure readability by specific machines or end users only.

Security holograms are microscopic relief patterns and hence cannot be photocopied. Holograms can hold different levels of security features. It is not easy to produce or reproduce a well-designed security hologram. Security holograms are produced and used in millions and always quick and effective primary verification of security holograms has been a challenge. Security holograms contain large amount of complex information and hence machine readability of security holograms has been a big challenge right from its introduction. Hence specific feature based primary authentication of security holograms is practiced globally. If barcodes are combined with security holograms, it is possible to have legal sanctity, machine readability, automation, secure tracking and tracing of a product or a document. However, it is difficult to directly incorporate individual holographic barcodes or other variable data in each security hologram embossed from the master. Hence if serial numbering or coding is to be added to security holograms, it is generally done through laser engraving or overprinting of the hologram.

11. Facts and fallacies of security holography

Even after decades of its introduction, security holograms are still topping the list of effective security devices and are widely applied across the world. There are various reasons for this. Failure of modern digital tools in effectively copying security holograms is one of the main reasons for its success. A highly dynamic technology front and emergence of new security features and new technologies is another reason for the success of security holograms. Security holograms are immensely cost effective and this proved another important fact that efficacy of a security project is not directly proportional to the cost involved. However, design of the hologram to disposal of rejections is of immense importance here. But, many companies produce security holograms just as a sticker with glitter. This is an important matter to be addressed. Leakage of a single hologram can hamper an entire project and a set of standards and procedures are to be strictly adhered to ensure efficacy of security holography. The end user and the hologram production company can have better control over the project and the security aspects if production of security holograms, right from mastering to waste disposal is done under single roof.

12. Is it possible to counterfeit security holograms?

Answer to this question must start with the basic assumption in security that anything manmade can be counterfeited. We are living in a technology era that witnessed replication of DNA, the most complex structure, and the building block of life. So, nothing prevents a counterfeiter to try production of fake holograms too. In fact if a security hologram is introduced on a product or a document, counterfeiters have three options left with them. They can stop counterfeiting and quit their illegal activities, which is quite unlikely in all practical cases. A second option is to get a copy of the high security master or original security holograms through illegal means. A set of production and security procedures can thwart the above possibility. Reusing the original holograms is a third option. Tamper evident holograms combined with modern ICT based tracking can nullify this possibility. As a fourth option counterfeiters can try to make 'look alike' holograms.

But, if the hologram master is well designed and implemented, it is virtually impossible to make effective look alike counterfeit holograms.

13. How ‘look alike’ holograms are made?

Reverse engineering and re-origination, copying from original hologram and re-mastering are some of the methods followed by the counterfeiters. In reverse engineering, a new counterfeit hologram master is created and this is used to produce fake holograms. A well designed security hologram contains truly complex submicron structures that yield several covert and overt optical features and in reality it is not an easy task to reverse engineer such a hologram. Hence reverse engineered counterfeit holograms can be identified with relative ease. On the other side, copying from the original and re-mastering make the situation a little tougher. There are optical and electro-mechanical methods to copy a micro structure. To make such methods ineffective, holographic micro-structures are generally embossed from bottom and kept protected under a thin tamper layer, coated with metal and this is again coated with the adhesive layer. Hence, if the counterfeiter tries to remove the hologram, the hologram will be damaged. Also, through advanced forensic verification, it is possible to identify such fake holograms.

14. Prevention of Reuse

Reuse of security holograms is another threat globally posed by the counterfeiters. Here either the packaging itself is reused to fill with counterfeit products and sell these to make easy money or the hologram is removed one by one and reapplied on the product. The latter method is not easy and effective with low value products. However, this can be effective with high value products such as alcoholic beverages, ID Cards and critical documents. Proper design of the master, design of the package or the substrate on which the hologram is applied, location of application of the hologram, design of proper production and security procedures etc. can effectively address the issue of counterfeit holograms. Role of a reliable production company with in-house mastering facility and state of the art knowledge and expertise is of utmost importance in security holography.

Thus well designed and well produced security holograms are still the most reliable global security device that can help governments and original manufacturers. So the belief that ‘Holograms are just low priced glittering stickers and they do not have much security value’ is just a fallacy.

15. A Few Interesting Examples

a. Liquor Tax Labels

Usually tax labels are applied on liquor and beer bottles to ensure that the tax is paid for a particular bottle containing liquor. These tax labels, applied on the bottle lid, overlapping with the bottle, not only authenticate that tax is paid and the product is from the original legal source, but act as a security seal for the content of the bottle. Tax content of liquor and such spirit based beverages are huge in many countries and amounts to even 300% of its actual production cost. So sales of counterfeit liquor are a golden avenue for many criminals. Nexus between political power centers and the counterfeiters make the enforcement and the entire legal system ineffective. In States where it is not legally permitted to sell loose liquor, counterfeiters are forced to produce fake liquor tax labels and apply these on bottles with illicit liquor and sell through various outlets. On the other hand, liquor sourced from original manufacturers will also be flooded into the market, after applying fake tax labels, so as to derive huge profit. A major part of the revenue inflow of many States is through liquor and cigarette tax collection and this amount to many billions of dollars. Thus in security design, production and distribution of liquor, this tiny label becomes highly important and technologically involved. If a tax evaded liquor bottle comes from an original manufacturer, chemical analysis will not prove its true authenticity and the enforcement fails miserably and the government will continuously fail in court cases and legal actions. Failure of governments will fuel the counterfeiting industry to move ahead with added confidence and dedicated officials will become frustrated. People will lose confidence in governance and the legal system itself.

b. ID Cards

Normal ID Cards contain a set of printed information, a photograph of the person and a stamped or pasted hologram. Smart ID Cards will contain an electronic chip. Generally at the entrance of an institution or a big complex of several companies where thousands of people work, the ID card of the card holder will be verified by the security official. Entry is permitted based on a visual comparison of the photograph with the actual person. The security personal may also ensure that the hologram is intact and primarily correct. If a proximity reader is there, the system will automatically detect the card and entry is permitted.

It is easy to overcome the above system and intrude into the premises. This is done by overprinting an existing ID card with another person's image. In a routine manner the security official or enforcement will verify the photograph of the card holder and the hologram and permit the intruder into the premises. If the data of the card is current, the proximity reader will also allow entry. This can lead to fatal security breach and severe damage. This is especially true with airports and software parks where thousands of employees from different countries function and it is personally difficult for the security to memorize all the staff. Biometric access control systems linked with ID Cards laminated with transparent holographic microstructures can make overprinting in effective and help a lot to address and detect such threats.

c. Bank Note Counterfeiting

Counterfeiting of Bank Notes is a big threat being faced by almost all of the countries, including the developed nations that have sophisticated technologies, strong legal system and a network of strong enforcement facilities. Basic testing of Bank Notes is done by feeling the paper and by verifying a few overt features. Compared to other documents, Bank Notes contain an ensemble of security features of different categories and sophistication levels. But, still bank notes are widely counterfeited by applying various techniques. Almost all of the printed features are duplicated by digital means. If the counterfeiter has access to banknote paper, it is not that challenging to create a sophisticated counterfeit that passes even a trained experienced person's primary testing. Some of the counterfeit Bank Notes are so identical that even the governmental system finds it difficult to correctly authenticate the Notes. Absence of high quality holograms and lack of advanced features with individual unique machine readable variable data are reasons for wide spread counterfeiting of Bank Notes. Currently security holograms and diffractive structures are introduced on both paper based and polymer based high denomination Bank Notes of many countries and this helped a lot in deterring counterfeiting. Introduction of individual unique machine readable variable data codes combined with a central secure database can make the system more effective and efficient. But, this needs great political will, international discussions, deliberations and policy making, since such next generation Bank Notes will become 'trackable'.

16. Importance of Security Procedures in Holography

Strict adherence to procedures are highly essential in any security related project and production. This is especially true with security holography too and right from design to production, and inspection to waste disposal, several security procedures are to be followed. Design of the Security Procedures is to be made by keeping in mind all the possible loopholes that the system can have, due to deliberate human efforts and accidental human and system errors. Security Threat Variables (STVs) of the system is to be listed and a Security Threat Index (STI) is to be assigned. A set of well-designed procedures will help a lot to have reduced STI for a particular system. Thus a near foolproof and reliable system can be achieved. Production companies with totally In-House production facility with own mastering system will help to achieve total control over the production of the security holograms. This is especially true with tax labels and critical high security holograms that are used globally. Total yearly turnover of certain products (say liquor, cigarettes, national IDs etc.) that are protected by the tiny holographic tax labels come to several billions of USD. So it is highly sensible for the governments to have own Fully In-house Security Hologram and Document Production Centers. This will help to achieve a small STI in the production and distribution of critical documents and products of much national and social importance.

17. Latest Trends and New Types of Security Holograms

Optical technologies and photonics now play a pivotal role most of the avenues of information communication technologies. Fusion of photonics and electronics can lead to a set of next generation high security solutions that can effectively fight with the global counterfeiting menace. Introduction of hologram integrated paper tax stamps and labels with linear or 2D barcodes is a typical example. This facilitated track and trace, advanced security, easy primary verification and simultaneous legal sanctity for original products and documents. Mastering and mass replication through embossing makes security holograms cost effective. Security holograms have much optical variability and look different in different angles. So they are termed as Optical Variable Devices (OVDs). However, present security holograms cannot hold machine readable holographic variable data that will make each security hologram distinct with its own secure machine readable identity. This was a major drawback of traditional security holograms and this was addressed through the introduction of laser or inkjet based serial numbering on the hologram. Emergence of Photopolymer holograms effectively addresses this lacuna by holding variable data. This can also facilitate possibility of advanced phase encryption.

Overt Data-matrix codes can be read by mobile phones and this helps to have widespread global primary verification based on a secure network and a database maintained by the original manufacturer or government. This adds scope for easy customer interaction and feedback. Machine readable holographic codes enhance the above security level by many folds. Mobile phones in conjunction with additional gadgets and custom application software unfolds a world of new possibilities.

Acknowledgement: Apart from first-hand experience and knowledge gained over three decades, this paper is an outcome of several discussions the author had over a period of time with globally renowned experts and professionals, working in the field of anti-counterfeiting and security technologies. It is difficult and not practical to name each and every one. So, the indebtedness of the author to the global community that works for the advancement of anti-counterfeiting technologies and strives for its effective implementation is thankfully acknowledged. For more information: ceo@lightlogics.in