EFFECTIVENESS OF STATIC SCRAMBLING VS DYNAMIC SCRAMBLING SYSTEMS A CLASSIFICATION METHOD

MICHAEL T. HAYASHI

PIONEER COMMUNICATIONS OF AMERICA, INC.
COLUMBUS, OHIO

ABSTRACT

Various scrambling systems have been introduced to the market place as a possible solution to the industry wide problem of theft of service. The effectiveness of scrambling is often a very confusing and difficult factor to determine. Classification of the various scrambling systems available today yeilds two basic forms -- static and dynamic. The effectiveness of the two varies depending upon the key signal and reference signal used in the descrambling process. Majority of scrambling systems are designed by slightly deviating from NTSC TV standards. Thus, from its initial design concept, these scrambling systems are vulnerable to pirate designs. Complete video encryption may certainly be the solution. However, the associated price is not affordable today. What compromises can be made to design an affordable ultimate scrambling system?

INTRODUCTION

Theft of service is a major concern for the entire cable industry. This concern has increased in proportion to the increase in value and quantity of products to be "stolen." Various methods of service protection have evolved in recent years, with more expected to surface. TV signal scrambling (as we all know) is one of the techniques used to deter potential theft of TV signals. It should be made clear that scrambling is merely a protective mechanism for premium TV pictures. TV signal scrambling is not a means to avoid other forms of service theft to which our industry is exposed. The operator will still need to contend with theft of hardware, hardware tampering and security of operation (installers), etc. However, with the considerable increase in consumer value of cable programming and the number of channels offered, cable signals must be protected.

This paper discusses specific aspects of all forms of TV scrambling/signal encoding. The flood of various scrambling methods being introduced -- RF vs baseband, sine wave sync vs gated sync, jamming, dynamic switching, random rate, encrypted scrambling, just to name a few -- can be very confusing, especially when one is attempting to judge the relative security provided by each method.

DEFINITION OF TV SIGNAL SCRAMBLING

From a technical perspective, a scrambling system has two purposes -- to prevent reception by "normal" television and to be capable of restoring the scrambled signal for reception by "normal" television. In the United States, television sets are designed to National Television System Committee (NTSC) standards. Therefore, deviation from the NTSC standard processing of the signal in most cases will accomplish scrambling. However, the term, "normal TV," provides its own share of confusion due to the technical advances in television receivers to accommodate such relatively unstable signal sources as home VTR's and video game machines. In addition there is cable ready, component TV, and digital TV. Scrambling methods, therefore, must be carefully chosen to be sure they introduce a scrambling factor beyond what the TV reciever may consider a tolerable variance from its standard (NTSC).

The subjective effectiveness of scrambling is another factor to consider when selecting a scrambling method. The tolerance level for a scrambled picture of someone recieving that picture "free" may be very high. Therefore, the scrambling level should be sufficient to render any TV picture received without a decoder subjectively unacceptable to an audience group, even if they are recieving it "free." Depending on program content, what one wants to see or hear will vary, making it very difficult to determine a guideline as what is acceptable scrambling in all cases.

The final factor in determining secure scrambling is the level of difficulty required to defeat the scrambling method. The level of difficulty is tied directly to the cost of preventing defeat. Obviously, the ideal is authorized descrambler would have the highest difficulty level possible at the lowest possible cost.

STATIC VS DYNAMIC SCRAMBLING SYSTEMS

Based upon method of application, TV signal scrambling or encoding can largely be classified into two major categories: static scrambling and dynamic scrambling.

Static scrambling processes the signal in a constant and predictable manner with respect to time. Dynamic scrambling, on the other hand, takes away the element of predictability within the scrambled signal itself. Dynamic scrambling is thus more secure in most cases than static scrambling forms because it introduces an added element to be decoded -- time.

In addition to the actual scrambling itself, all active scrambling systems may incorporate one or two types of information for proper descrambling. A reference signal may be required to re-establish proper descrambling levels and/or timing. A key signal may be used to determine when and what type of encoding method may be taking place. In certain instances, the same signal may carry both two types of information creating a situation where the signal function can be easily misinterpreted or misunderstood.

Obviously, knowing the built-in reference/key signals is vital to decoding dynamic scrambling systems. This knowledge is not absolutely essential in static systems since ^ reference can be recreated once the scrambling method is determined. Thus, in a static system, a potential pirate designer has a choice of generating his own reference signal or utilizing the reference signal available within the scrambling system; whereas, in a dynamic scrambling system, the pirate designer is forced to retrieve the reference signal to descramble, restricting his choice of approach.

One variation of the static system is the combining of static form of scrambling with a varying reference signal. This method would seem to provide added security due to its protected reference signal, but it is essentially still weak due to the fact that the actual scrambling mechanism is static. Dynamic scrambling with an unprotected reference signal is likewise not absolutely secure once the relationship between the reference signal and the scrambled picture is established.

This brings us to the combination of dynamic scrambling and protected reference/key signal. To steal service, a pirate designer will now have to determine how the reference/key signal is protected. This type of scrambling system depends greatly on two factors -- the "dynamic"-ness of the scrambling method itself and the level of reference/key signal protection. Dynamic scrambling, as we determined earlier, depends on the level of upredictability with respect to timing of the scrambling itself. Perhaps it would be more understandable to say that the larger the number of possible scrambling patterns or modes, the more unpredictable the system will be. No matter how dynamic the signal, the scrambling system itself loses its effectiveness against pirate designers if the reference signal is easily decoded. Therefore, analogue protection of reference signal with its limited number of variations is not as desirable as digital encoding which potentially has a significantly greater number of combinations.

In order to better understand the differences in static vs dynamic scrambling and the relationship to reference/key signal, let us look at a generic example.

A TV picture consists of synchronization pulses required to center the picture onto its CRT. Elimination of these pulses theoretically causes scrambling by preventing the TV set from stabiling the picture. Sine-wave sync suppression systems and gated sync suppression systems are all designed to achieve this effect. For the sake of illustration, let us use sync suppression for our exercise design of a secure scrambling system.

The first form we might use is constant video sync suppression with a fixed reference signal AM modulated on the aural carrier. Refering to our definition, this method is static scrambling in its most basic form. The second step we may take is to vary the reference signal timing so it does not corelate to the actual sync suppression timing. Still, the scrambling is a constant video sync suppression which is static. It is therefore, vulnerable to pirate design by bypassing the reference signal all together. Understanding that even a varying reference signal does not adequately protect a scramble picture because it can be bypassed, we can probably safely conclude that all forms of static scrambling offer approximately the same amount of protection from pirate designs.

Dynamic scrambling when applied to sync suppression offers a wide variety of scrambling combinations. Alteration of the depth of sync suppression, variation of the suppression frequency in a manner that makes it a harmonic of the sync frequency, random sync suppression by frame and random sync suppression by line, all have the potential to qualify as dynamic scrambling if they meet the criteria of unpredictability with respect to time. These methods are in many cases an improvement over static methods. However, even here an unprotected reference signal makes dynamic scrambling just as vulnerable to theft as static systems. For example, if the timing information for random sync suppression were directly AM modulated on the aural carrier, all the pirate would have to do is reapply that signal to the scrambled video. The timing reference for random sync suppression can be digitized. A digital data word corresponding to suppressed or not suppressed is an added layer of protection requiring data detection and decoding. Although considerably more secure than our starting point of basic static sync suppression, there is still a vulnerability factor in the "dynamic"-ness of the scrambling method and the decoding of the reference signal.

ENCRYPTION DEFINITION AND POTENTIAL

A constant "game" is currently being played in the cable industry with regard to theft of signal. One day a very powerful scrambling method is announced. The next day it is defeated. The cable operator wants a secure signal, but cannot relay on claims made because pirate designers are keeping up with the pace of vendor technology. In an environment like this, encryption of signal is an ideal form of signal protection. Encryption technology assumes, given time, all codes, will eventually be broken. This is philosophy recognizes the present scrambling games played between the pirate designers and the cable industry. The difference is that most encryption systems allow an astronomical number of variations for possible key codes to the encrypted signal. An anology can be made to a door lock and its key. The mechanism of a door lock is common knowledge; however, if you do not have the key that fits, you will not be able to open that door lock. Suppose you finally duplicated the key by carefully studying the door lock, but that lock can be easily changed to let a different key work. . . . The door lock is like a scrambling method which can be made public knowledge because there are a billion variations of possible keys and the internal components of the lock are continually changing.

The advantages of scrambling systems using encryption are numerous. Descrambling devices could be sold directly to the subscriber without fear that they would be used as a potential theft tool. The majority of today's pirate devices are add-on descrambling bases made up of actual manufacturers' products which have been either stolen or sold indirectly to the pirate houses. If the descrambler can be properly activated only by entering a unique key code which will vary from time and which is given only to paying subscribers, problems associated with the distribution of descramblers can potentially be solved.

The benefits of descrambler standardization as a result of encryption, coupled with TV standardization, may eventually allow the cable operator to eliminate a significant amount of hardware investment in the home. Of course, the operational aspect of this possibility will have to be carefully studied. With cable penetration over the 35% mark, making the descrambler a direct consumer product is not an unreasonable proposal. Encryption algorithm must be chosen so that it allows viewing only by a valid paying subscriber. The problem of paying subscribers disclosing encryption keys must be resolved both in operational system design and hardware design. A customized unique decrypting number for specific subscriber hardware may exist on a monthly billing basis, service basis, or even per program basis.

Now that we have seen a some idea of what encryption can possibly do for us, we can explore what is to be encrypted. Let us continue the evolution of the product design we started in our earlier appraisal of static scrambling. Our next step will be to encrypt the key signal associated with a dynamic scrambling method. If random sync suppression within a TV picture frame were the dynamic scrambling method chosen, the suppressed or not-suppressed timing is encrypted. Detection of digital key signal cannot be used to directly decipher the random occurrences of sync suppression unless the algorithm and decryption code are determined.

This form scrambling is particularily powerful since a decryption code may have a million possible combinations in addition to the dynamically changing patterns of sync suppression. In addition to the signal security of dynamic scrambling, encryption of key signal now provides opportunity to design systems which could safely allow standalone descramblers. The descramblers in this type of system could be made unique relative to each other. Changes in algorithm factors from systems to system will automatically resolve the cross system theft problem.

The last step in this design exercise is to encrypt video content. So long as the scrambled information does not alter basic video information, all non-encrypted video scrambling methods carry the possibility of being defeated. A variety of methods exists for encrypting video. These methods range from a simple a simple line randomization to time randomization of picture content, just short of digital video transmission.

STATE OF TECHNOLOGY

A true encrypted scrambling system is currently only available to the satellite industry due to the cost associated with encrypted scrambling. Satellite descramblers can afford to carry a price tag of several thousand dollars. Scramble/ descramble systems for the CATV industry certainly will have to maintain current price levels, eliminating direct application of satellite descramblers in the home. However, with the advent of charge coupled device (CCD) technology, digital television technology and advances in other semiconductor technology, the cost associated with complicated video processing can significantly drop, and true encrypted scrambling may some day be a viable technique for CATV signal protection.

Probably the most advanced form of scrambling systems available today within a competitive price range are the hybrid systems which use dynamic scrambling and encrypted digital key codes. Certainly not expected to last forever undefeated as long as these systems are designed within the realm of NTSC standards. Dynamic scrambling methods all maintain the basic rules set forth in the NTSC standards. For example, the deviation from NTSC standards of sync suppression and video inversion are relatively very minor. Significant deviation is not possible from the reasons associated to cost of product and ease of design. And for the very same reason, the vulnerability to pirate designers remains.

CONCLUSION

Scrambling system as they exist today are certainly not the ultimate solution to theft of service. The degree of difficulty in descrambling may vary from method to method; however, no metnod available to the industry can guarantee it will never be defeated. Some new TV sets are designed to be capable of tuning to semi-scrambled signals. Certain TV sets, for example, can automatically descramble static sync suppression. Less simple but a likely possibility for defeating all regular scrambling systems including dynamic scrambling, are other modification method using the TV set as a descrambling tool. Such modifications are possible since descramblers, to be price competitive, are designed with components commonly found insider the TV set itself.

Furthermore, many scrambling systems do not take into consideration other factors which impact theft of service. A system may develop a very powerful secure scrambling method which is ultimately defeated because it is housed in a descrambler device which lacks proper hardware security.

Theft of service can be greatly reduced by eliminating incentives that induce theft. Hardware construction of descrambler units should be secure to protect the internal components. Mechanical locks, access traps, custom chips, etc., should be used. Even the all outdoor delivery methods base signal security on lack of incentive for a potential thief to climb a pole or break a pad lock to steal service. While secure scrambling is certainly desireable, it is often overemphasized in the total theft of service scene. Strong scrambling methods are needed but equal attention must be placed on the operational aspect of the design so that the incentive to steal is eliminated.

Similarly, scrambling methods should minimize theft incentives. However, all video scrambling methods available to the cable industry today are only minor deviations from the NTSC standards, and thus, remain vulnerable to pirate designs. The issue is then the relative strength of the system against pirate designs. The question remains to be answered as to how much value does an ultimate scrambling system, designed within the realm of minor deviation from NTSC standard, have. Today, short of complete video encryption, the dynamic scrambling with encrypted key signal is most secure alternative one can offer.